



GFI Product Manual

GFI LanGuard™

*Administration and Configuration
Manual*



<http://www.gfi.com>
info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI LanGuard 2011 is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Last updated: August 12, 2011

Version: LANSS-ACM-EN-01.00.01

Contents

1	Introduction	1
1.1	Introduction to GFI LanGuard	1
1.2	About this manual	1
1.3	GFI LanGuard components.....	3
1.4	Vulnerability management strategy.....	4
2	Managing Agents	5
2.1	Introduction	5
2.2	Deploying agents.....	5
2.3	Configuring Agents.....	8
3	Agent-less Auditing	11
3.1	Introduction	11
3.2	Performing a manual audit	11
3.3	Scheduled scan.....	16
3.4	Setting up scheduled scans.....	17
3.5	Audit result summary	23
3.6	Audit result details	26
4	Analyzing Results	37
4.1	Introduction	37
4.2	Computers view	43
4.3	History view	45
4.4	Vulnerabilities view	46
4.5	Patches view.....	47
4.6	Ports view.....	48
4.7	Software view	49
4.8	Hardware view	50
4.9	System Information.....	51
4.10	Display results.....	51
4.11	Configure credentials	52
4.12	Monitoring activity.....	53
5	Fixing Vulnerabilities	57
5.1	Introduction	57
5.2	Automatic-Remediation.....	57
5.3	Remediation center	65
5.4	Deploy security patches and service packs	67
5.5	Uninstall software patches and service packs	68
5.6	Deploy custom software	69
5.7	Uninstall custom applications.....	71
5.8	Malware protection actions	72
5.9	Using remote support	73
5.10	Remediation Jobs.....	74

6	Configuring GFI LanGuard	77
6.1	Introduction	77
6.2	Scheduled Scans.....	77
6.3	Applications inventory	79
6.4	Configuring security updates.....	83
6.5	Configuring alerting options.....	87
6.6	Database maintenance options	88
6.7	Program updates	93
6.8	Importing and Exporting Settings.....	97
7	Reporting	103
7.1	Introduction	103
7.2	Available reports.....	103
7.3	Generating reports	105
7.4	Custom reports.....	108
7.5	Full text searching.....	110
8	Scanning Profiles	113
8.1	Introduction	113
8.2	Scanning profile description.....	113
8.3	Configure Vulnerabilities Assessment options	117
8.4	Configure Network & Software Audit options.....	126
8.5	Configuring the security scanning options	137
9	Utilities	139
9.1	Introduction	139
9.2	DNS lookup.....	139
9.3	Traceroute.....	141
9.4	Whois	142
9.5	Enumerate computers.....	143
9.6	Enumerate users	145
9.7	SNMP Auditing	146
9.8	SNMP Walk	147
9.9	SQL Server Audit	148
10	Using GFI LanGuard from the command line	149
10.1	Introduction	149
10.2	Using the command line scanning tool: Insscmd.exe.....	149
10.3	Using the command line patch deployment tool: deploycmd.exe.....	150
10.4	Using the command line import and export tool: impex.exe	151
11	Adding vulnerability checks	153
11.1	Introduction	153
11.2	GFI LanGuard VBscript language.....	153
11.3	GFI LanGuard SSH Module	155
11.4	Python scripting.....	159

12 GFI LanGuard certifications	161
12.1 Introduction	161
12.2 About OVAL	161
12.3 About CVE.....	162
13 Miscellaneous	165
13.1 Enabling NetBIOS on a network computer.....	165
14 Troubleshooting	167
14.1 Introduction	167
14.2 Common Issues	167
14.3 The Troubleshooting wizard.....	169
14.4 Knowledge Base	171
14.5 Web Forum.....	171
14.6 Request technical support.....	171
14.7 Build notifications	172
15 Glossary	173
16 Appendix - Data Processed by GFI LanGuard	177
16.1 Introduction	177
16.2 System Patching Status	177
16.3 Ports	177
16.4 Hardware.....	178
16.5 Software.....	179
16.6 System Information.....	180
Index	183

List of tables

Table 1 -Target selection	6
Table 2 - Automated network audit properties	6
Table 3 -Add new rule	7
Table 4 -Agents settings	8
Table 5 - Target options when auditing	12
Table 6 - Logon and audit options	13
Table 7 - Scan Results	14
Table 8 - Custom target properties	15
Table 9 - New scheduled scan type	17
Table 10 - Remote logon credentials	19
Table 11 - Auto-remediation options	20
Table 12 - Reporting options	21
Table 13 - Response time icons	27
Table 14 - GFI LanGuard Vulnerability groups	27
Table 15 - System patching status	30
Table 16 - Hardware information from an audit	31
Table 17 -Software information from an audit	31
Table 18 - System information from an audit	32
Table 19 - Agent status	39
Table 20 - View by computers information	43
Table 21 - Authentication methods	53
Table 22 - Updates download status	55
Table 23 - Security updates download	55
Table 24 - Automatic remediation actions	57
Table 25 - Automatic remediation stages	57
Table 26 - Before deployment	60
Table 27 - After deployment	61
Table 28 - Advanced deployment options	62
Table 29 - Advanced deployment options	63
Table 30 - Warning messages	64
Table 31 - Remediation actions	66
Table 32 - Options available in Deploy Custom Software	70
Table 33 - Launch deployment options	71
Table 34 - Uninstall options	72
Table 35 - Options to manage scanning profiles	77
Table 36 -Schedule scan properties	79
Table 37 - Manage applicable schedule scans	83
Table 38 - Mail settings parameters	87
Table 39 - Database retention options	93
Table 40 - Proxy settings	94
Table 41 - Override options	101
Table 42 - Available reports	103
Table 43 - Customize report parameters	108
Table 44 - Report placeholders	110
Table 45 - Complete/Combination scanning profiles	113
Table 46 - Vulnerability assessment scanning profiles	114
Table 47 - Network and Software audit scanning profiles	114
Table 48 - Vulnerability properties dialog	119
Table 49 - Applications Options	134
Table 50 -DNS lookup options	140
Table 51 - Insscmd command switches	149
Table 52 - Supported variables in inssmcd	150
Table 53 - deploycmd command switches	150
Table 54 - impex command switches	151
Table 55 - GFI LanGuard common issues	167
Table 56 - Information gathering options	170

List of screenshots

Screenshot 1 - GFI LanGuard script debugger	3
Screenshot 2 - Home page	5
Screenshot 3 - Manage agents	6
Screenshot 4 - Deploy agent wizard	7
Screenshot 5 - Agent properties	9
Screenshot 6 - Agent auto-remediation	10
Screenshot 7 - Launch manual scan	12
Screenshot 8 - Manual scan settings	12
Screenshot 9 - Scan result details	14
Screenshot 10 - Custom target properties	15
Screenshot 11 - New Scheduled Scan dialog	17
Screenshot 12 - Scheduled scan frequency	18
Screenshot 13 - Select scanning profile	18
Screenshot 14 - Remote logon credentials	19
Screenshot 15 - Scheduled scan auto-remediation options	20
Screenshot 16 - Scheduled scan reporting options	21
Screenshot 17 - Review scheduled scan job	22
Screenshot 18 - Scheduled scan status	22
Screenshot 19 - Scan summary	23
Screenshot 20 - Vulnerability level meter	24
Screenshot 21 - Reloaded scan results	25
Screenshot 22 - Detailed view tab	26
Screenshot 23 - The Vulnerability Assessment node	27
Screenshot 24 - Missing Service pack: Bulletin info dialog	29
Screenshot 25 - The network and software audit node	29
Screenshot 26 - System patches status	30
Screenshot 27 - All UDP and TCP ports, found during a scan	30
Screenshot 28 - The audit policy administration wizard	34
Screenshot 29 - Results dialog in audit policy wizard	34
Screenshot 30 - View Dashboard	37
Screenshot 31 - Network Security Level	38
Screenshot 32 - Computer Vulnerability Distribution	38
Screenshot 33 - Most Vulnerable Computers	38
Screenshot 34 - Agent Status when selecting a domain/workgroup	39
Screenshot 35 - Audit status chart	39
Screenshot 36 - Vulnerability Trends Over Time for a domain/workgroup	40
Screenshot 37 - Vulnerability Trends Over Time for a single computer	40
Screenshot 38 - Computers by network role	40
Screenshot 39 - Computers by operating system	41
Screenshot 40 - Computer Details	41
Screenshot 41 - Scan activity	41
Screenshot 42 - Remediation activity	42
Screenshot 43 - Top 5 issues to address	42
Screenshot 44 - Result statistics	42
Screenshot 45 - Analyze results by computer	43
Screenshot 46 - Dashboard: History	45
Screenshot 47 - Dashboard: Vulnerabilities	46
Screenshot 48 - Dashboard: Patches	47
Screenshot 49 - Dashboard: Ports	48
Screenshot 50 - Dashboard: Software	49
Screenshot 51 - Dashboard: Hardware	50
Screenshot 52 - Dashboard: System information	51
Screenshot 53 - Dashboard filtering criteria	52
Screenshot 54 - Computer\Domain list	52
Screenshot 55 - Configuring computer credentials	53
Screenshot 56 - Action Center: Scheduled Activity	54
Screenshot 57 - Security updates download	55
Screenshot 58 - Product updates activity	56
Screenshot 59 - Application inventory	58
Screenshot 60 - Mark application as unauthorized	59
Screenshot 61 - Before deployment options	60

Screenshot 62 - After deployment options	61
Screenshot 63 - Advanced deployment options	62
Screenshot 64 - Reboot/shut down options	63
Screenshot 65 - Warning messages	64
Screenshot 66 - Remediation center	66
Screenshot 67 - Select the updates to deploy	67
Screenshot 68 - Deploying missing patches on selected computers	67
Screenshot 69 - Deploy patches	68
Screenshot 70 - Uninstall security patches	69
Screenshot 71 - List of software to be deployed	70
Screenshot 72 - Target computers for software deployment	70
Screenshot 73 - Launch deployment options	70
Screenshot 74 - Uninstall applications	71
Screenshot 75 - Malware protection	72
Screenshot 76 - Remote desktop connection	73
Screenshot 77 - Remote desktop connection	74
Screenshot 78 - Remediation jobs	75
Screenshot 79 - Scheduled scans	77
Screenshot 80 - Scheduled scan toolbar	77
Screenshot 81 - Scheduled Scan properties	78
Screenshot 82 - Configuring Applications inventory	79
Screenshot 83 - Unauthorized application - scanning profile	80
Screenshot 84 - Applications inventory wizard	81
Screenshot 85 - Application auto-uninstall validation	82
Screenshot 86 - Manage applicable schedule scans	83
Screenshot 87 - Patch auto-deployment	84
Screenshot 88 - Patch Auto-Deployment Advanced Options	85
Screenshot 89- Configuring Patch Auto-download Properties	86
Screenshot 90 - Configuring Alerting Options	87
Screenshot 91 - The database maintenance properties dialog	88
Screenshot 92 - Microsoft SQL Server database backend options	89
Screenshot 93 - Database maintenance properties: Managed saved scan results tab	90
Screenshot 94 - Database maintenance properties: Scanned Computers tab	91
Screenshot 95 - Database Maintenance properties: Advanced tab	92
Screenshot 96 - Program updates	93
Screenshot 97 - Configuring proxy server settings	94
Screenshot 98 - Configure updates at application startup	95
Screenshot 99 - The Check for Updates wizard: Stage 1	96
Screenshot 100 - The Check for updates Wizar	97
Screenshot 101 - Import and Export Configuration	98
Screenshot 102 - Export configurations to file	98
Screenshot 103 - Import and Export Configurations	99
Screenshot 104 - Import configurations from a file	99
Screenshot 105 - Import and Export Configurations	100
Screenshot 106 - Import setting	100
Screenshot 107 - Reporting tab	103
Screenshot 108 - Report sample	106
Screenshot 109 - Scheduled reports settings	107
Screenshot 110 - Customize the report parameters	108
Screenshot 111 - Customize the report parameters	111
Screenshot 112 - Launch the scanning profiles editor	115
Screenshot 113 - The Scanning Profile Editor	116
Screenshot 114 - Scanning Profiles properties: Vulnerabilities tab options	117
Screenshot 115 - Select the vulnerability checks to be run by this scanning profile	118
Screenshot 116 - Vulnerability properties dialog: General tab	119
Screenshot 117 - Vulnerability conditions setup tab	120
Screenshot 118 - Check properties wizard	121
Screenshot 119 - Edit vulnerability	122
Screenshot 120 - Advanced vulnerability scanning dialogs	123
Screenshot 121 - Scanning Profiles properties: Patches tab options	124
Screenshot 122 - Select the missing patches to enumerate	125
Screenshot 123 - Searching for bulletin information	125
Screenshot 124 - Extended bulletin information	126
Screenshot 125 - Scanning Profiles properties: TCP Ports tab options	126

Screenshot 126 - Scanning Profiles properties: UDP Ports tab options	128
Screenshot 127 - Scanning Profiles properties: System Information tab options	129
Screenshot 128 - The network devices configuration page	130
Screenshot 129 - Advanced network devices configuration dialog	131
Screenshot 130 - The Devices configuration page: USB Devices tab options	132
Screenshot 131 - The applications configuration page	133
Screenshot 132 - The Applications tab: Installed Applications tab options	134
Screenshot 133 - The Applications configuration page: Advanced Options	135
Screenshot 134 - Security Applications Alert Configuration	137
Screenshot 135 - Scanning Profiles properties: Scanner Options tab	138
Screenshot 136 - The DNS Lookup tool	139
Screenshot 137 - The DNS Lookup tool	140
Screenshot 138 - Trace route tool	141
Screenshot 139 - Whois tool	142
Screenshot 140 - Enumerate Computers tool	143
Screenshot 141 - The Enumerate Users tool dialog	145
Screenshot 142 - SNMP Audit tool	146
Screenshot 143 - SNMP Walk	147
Screenshot 144 - SQL Server Audit	148
Screenshot 145 - The new vulnerability check dialog	154
Screenshot 146 - The check triggering conditions dialog	155
Screenshot 147 - The check triggering conditions dialog	158
Screenshot 148 - Independent checks: Python Script Test	159
Screenshot 149 - Searching for CVE information	163
Screenshot 150 - Local Areas Connection properties: WINS tab	165
Screenshot 151 - Troubleshooter wizard - Information details	169
Screenshot 152 - Troubleshooter wizard - Gathering information about known issues	170
Screenshot 153 - Troubleshooter fixed known issues	171

1 Introduction

1.1 Introduction to GFI LanGuard

GFI LanGuard is a security scanning, network auditing and remediation solution that enables you to scan and protect your network through:

- » Identification of system and network weaknesses via a comprehensive vulnerability check database. This includes tests, based on OVAL, CVE and SANS Top 20 vulnerability assessment guidelines.
- » Auditing of all hardware and software assets on your network, enabling you to create a detailed inventory of assets. This goes as far as enumerating installed applications as well as devices connected on your network.
- » Automatic download and remote installation of service packs and patches for Microsoft operating systems and third party products as well as automatic un-installation of unauthorized software.

1.2 About this manual

This manual is a comprehensive guide aimed at assisting you in configuring and using GFI LanGuard. It builds on the instructions in the GFI LanGuard 'Getting Start Guide' and describes the use and configuration required to achieve the best possible results. The GFI LanGuard Getting Started Guide is available from:

<http://www.gfi.com/lannetscan/manual>

This manual contains the following chapters:

CHAPTER	DESCRIPTION
Chapter 1	Introduction Introduces this manual and GFI LanGuard.
Chapter 2	Managing Agents Provides information on how to deploy agents on your network.
Chapter 3	Agent-less Auditing Provides information on how to perform a manual and a scheduled scan without using GFI LanGuard agent. This chapter also includes information on how to view audit results.
Chapter 4	Analyzing Results Provides information on analyzing audit results using the status dashboard and the security sensors.
Chapter 5	Fixing Vulnerabilities Provides information on how to fix vulnerabilities, using automatic remediation, remediation centre and remote support.
Chapter 6	Configuring GFI LanGuard Provides information on how to customize and configure advanced settings in GFI LanGuard.
Chapter 7	Reporting Provides information on how to generate audit result reports and a description of the report contents.

CHAPTER	DESCRIPTION
Chapter 8	Scanning Profiles Provides information on the different scanning profiles in GFI LanGuard.
Chapter 9	Utilities Describes each utility in GFI LanGuard and how these can be used on your network.
Chapter 10	Using GFI LanGuard from the command line Describes the command line tools available in GFI LanGuard and how these can be used.
Chapter 11	Adding vulnerability checks Provides information on how to add vulnerability checks using VBscript and Python. Also includes information on GFI LanGuard SSH module.
Chapter 12	GFI LanGuard certifications Provides information on GFI LanGuard certifications, These include OVAL and CVE.
Chapter 13	Miscellaneous Provides information on how to enable NetBIOS on network computers
Chapter 14	Troubleshooting Provides information all the necessary information on how to deal with common problems encountered while using GFI LanGuard.
Glossary	Glossary Defines technical terms used within GFI LanGuard.
Appendix	Data processed by GFI LanGuard Provides information on the data processed by GFI LanGuard including ports and protocols used.

1.2.1 Terms and conventions used in this manual

The following table contains a description of the common terms and conventions used in this manual:

TERM	DESCRIPTION
	Additional information and references essential for the operation of GFI LanGuard.
	Important notifications and cautions regarding potential issues that are commonly encountered.
	Step by step navigation instructions to access a function.
Bold text	Indicate a control within the user interface, such as nodes, menus and buttons.
<i><Italic text></i>	Replace text within angle brackets. Such as file paths and custom parameters.
<code>Indented code</code>	The indented text indicates that the text is a programming code. In some programming languages indentation is important.

For any technical terms and their definitions as used in this manual, refer to the [Glossary](#) chapter.

1.3 GFI LanGuard components

GFI LanGuard's architecture is designed for performance reliability and scalability, which caters for medium to large networks.

GFI LanGuard consists of the following components:

GFI LanGuard management console

The management console enables you to configure and use GFI LanGuard 2011. It also enables you to analyze audit results.

GFI LanGuard attendant service

GFI LanGuard attendant is the background service that manages all scheduled operations including scheduled network security scans, patch deployment and remediation operations.

GFI LanGuard agent deployment

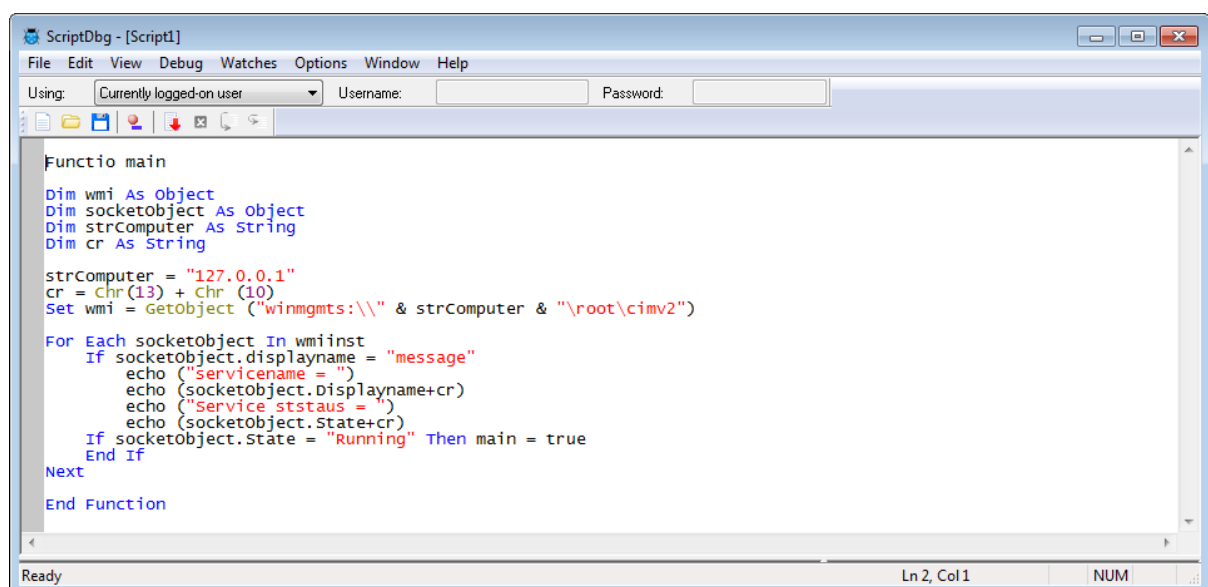
GFI LanGuard provides you with the facility to use agents. These enable real time result analysis and reduce network bandwidth consumption. Depending on how you configure GFI LanGuard, agents are deployed automatically on newly discovered machines or on manually selected computers. For more information on GFI LanGuard Agents, refer to [Managing Agents](#) chapter in this manual.

GFI LanGuard patch agent service

GFI LanGuard patch agent is the background service that handles the deployment of patches, service packs and software updates on target computers.

GFI LanGuard Script Debugger

The GFI LanGuard Script Debugger is the module that allows you to write and debug custom scripts using a VBScript-compatible language.



Screenshot 1 - GFI LanGuard script debugger

Use this module to create scripts for custom vulnerability checks through which you can custom scan network targets for specific vulnerabilities.

GFI LanGuard script debugger is accessible from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard Script Debugger**.

1.4 Vulnerability management strategy

GFI recommends you to follow the sequence below for an effective vulnerability management strategy:

1. **Configure Agents** - For more information, refer to [Managing Agents](#) section in this manual.
2. **Analyze** - For more information, refer to [Analyzing results](#) section in this manual.
3. **Remediate** - For more information, refer to [Fixing vulnerabilities](#) section in this manual.



Using agents is highly recommended because they provide real-time result analysis and reduce network bandwidth consumption. Agent-less audit is also available in GFI LanGuard. This enables you to perform audits manually or repeatedly on a schedule. For more information on Agent-less auditing, refer to [Agent-less auditing](#) section in this manual.

Important notes

1. In most cases, vulnerability scans generate different event log entries across diverse systems. Example, UNIX logs and web server logs will all detect GFI LanGuard scans as intrusion attempts triggered from the computer running GFI LanGuard.
2. For large network environments, a Microsoft SQL Server/MSDE database backend is recommended instead of the Microsoft Access database. For more information on how to configure the database backend, refer to [Selecting a database backend](#) section in this manual.
3. When submitting a list of target computers from file, ensure that file contains only one target computer name per line.



If Intrusion Detection Software (IDS) is running during an audit, GFI LanGuard will set off a multitude of IDS warnings and intrusion alerts in these applications. If you are not responsible for the IDS system, make sure to inform the person in charge about any planned security audits.



To perform an audit, GFI LanGuard must remotely logon to target computers with administrator privileges.



Agent deployment can only be done on Microsoft Windows operating systems.

2 Managing Agents

2.1 Introduction

GFI LanGuard can be configured to deploy live agents automatically on newly discovered machines or on manually selected computers. Agents enable data processing and auditing to be done on target machines; once an audit is finished, the result is sent to GFI LanGuard. Agents will:

- » Reduce scanning time
- » Minimize bandwidth consumption
- » Provide real time results



Agents can only be deployed on Microsoft Windows operating systems.

2.2 Deploying agents

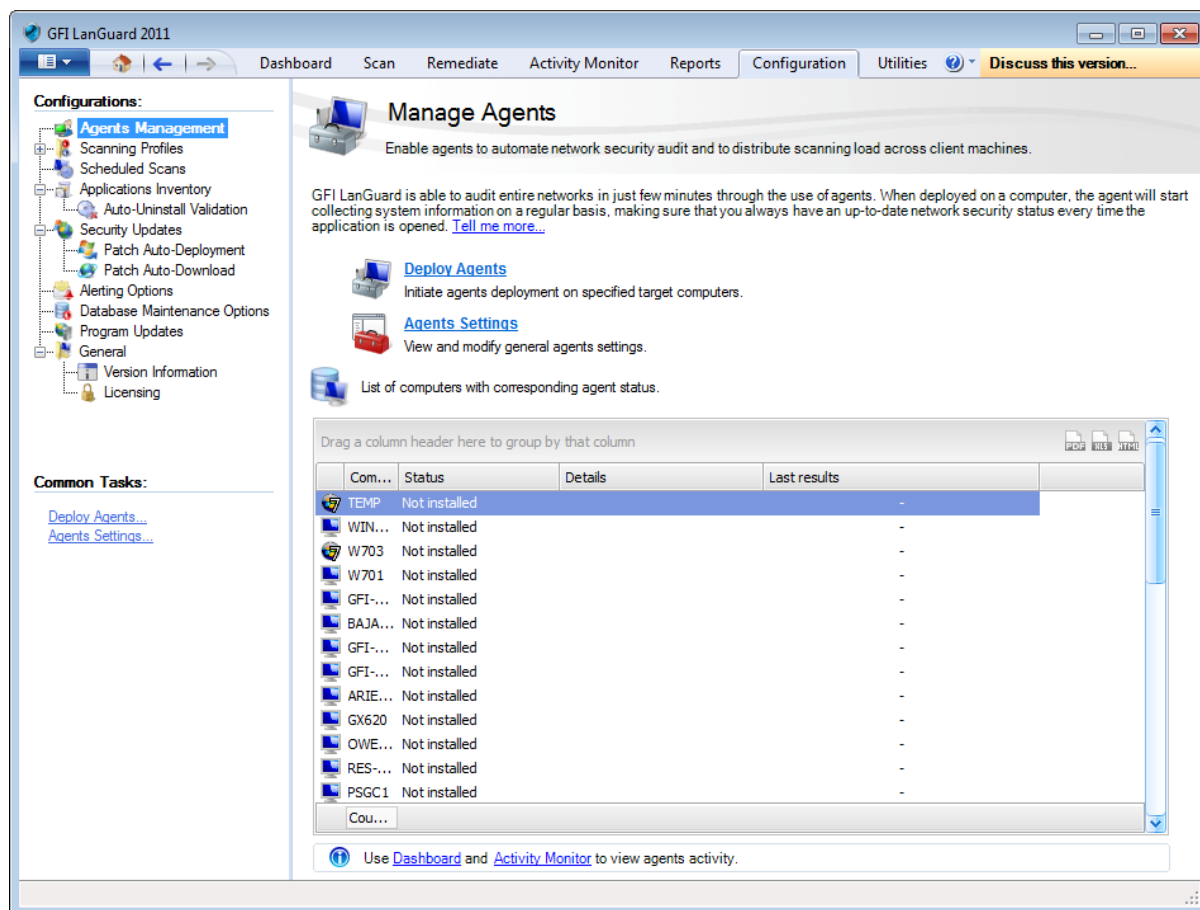
To configure agent's deployment:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**



Screenshot 2 -Home page

2. From the Home menu, select **Manage Agents**.



Screenshot 3 - Manage agents

3. Select **Deploy Agents** to select the target scan computers and click **Next**. There are two methods of selecting target computers, described below:

Table 1 -Target selection

OPTION	DESCRIPTION
Local Domain	Deploy agents on all reachable computers within the same workgroup / domain where LanGuard is installed.
Custom	Deploy agents on specific computers or group of computers. Add new rules to search or specify target scan computers. For more information on how to add new rules refer to the Custom Agent Deployment section of the manual.

4. (Optional) Select **Authenticate using** checkbox to specify alternate credentials.

5. (Optional) Click **Advanced Settings** to configure automated network audit properties. Table 2 below describes these automated network properties:

Table 2 - Automated network audit properties

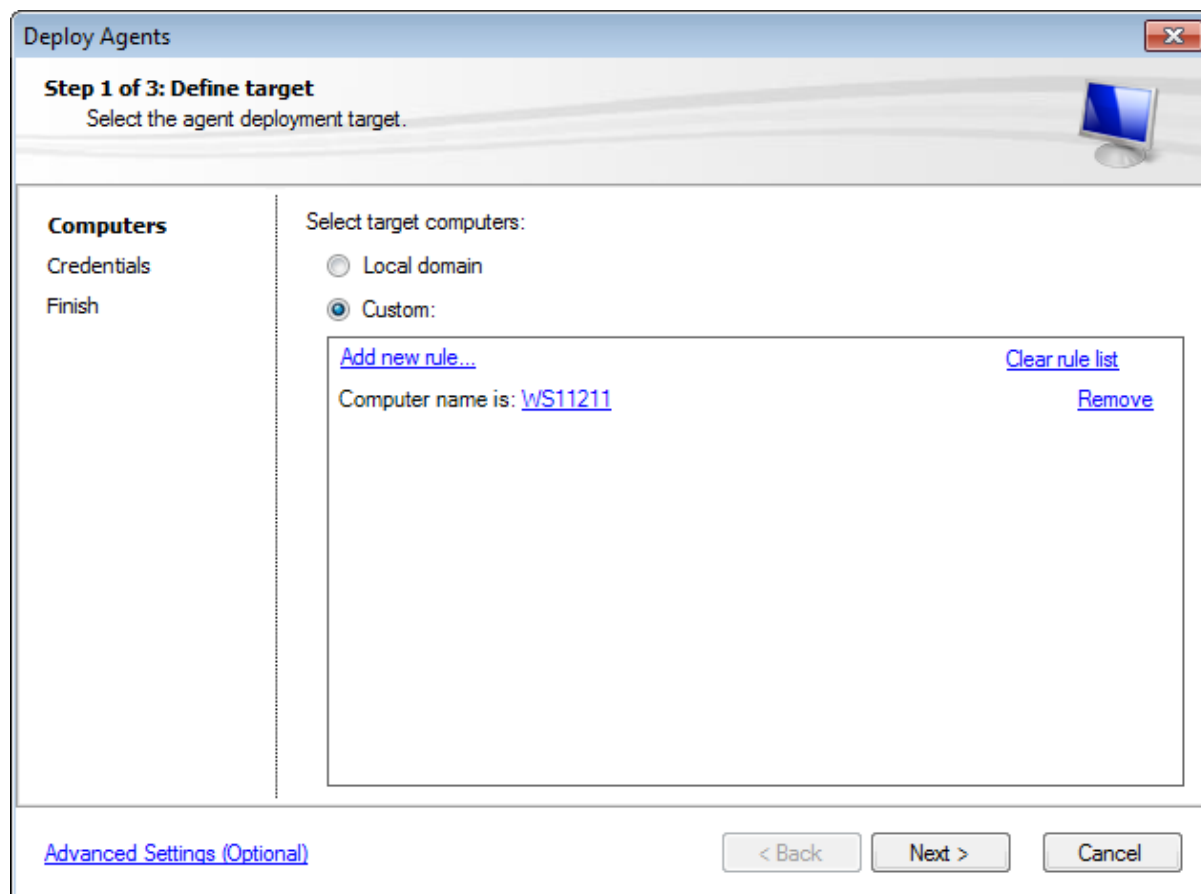
TAB NAME	DESCRIPTION
General	Configure the schedule for when GFI LanGuard automatically scans for new machines in the network perimeter where agents are enabled.
Audit schedule	Configure how often the agent audits the host computer (where the agent is installed). Select the recurrence pattern and the time the audit will start.
Auto-remediation	Configure GFI LanGuard to automatically download and install missing patches and service packs. Uninstall unauthorized applications on the scanned computers. For more information on how to configure auto-remediation, refer to Automatic Remediation section in this manual

6. Click **Next** and **Finish** to complete agent deployment.

	Alternate credentials must have administrative permissions on the scan targets.
	It is recommended to enable System Restore on the target scan computers if Auto-remediation is enabled in GFI LanGuard.

2.2.1 Custom agent deployment

The **Custom** option in the **Deploy Agents** wizard enables the creation of rules enabling you to search for specific computers. To launch the **Add new rule** dialog:



Screenshot 4 - Deploy agent wizard

1. Select **Custom** from the **Deploy Agents** wizard.

2. Click **Add new rule...**

Table 3 below describes the available options:

Table 3 -Add new rule

OPTION	DESCRIPTION
Rule type	Enables you to specify the target computers to scan. Select: » Computer name is - manually enter a computer name or import the names from a saved text (.txt) file. » Domain name is - select computers from one or more reachable domains. » Organization unit is - select computers from one or more reachable organization units.
Add	Add specified computer name to list.
Remove	Remove selected computer from list.

OPTION	DESCRIPTION
Select...	Select where to deploy agents from a list of reachable computers.
Import...	Specify location of a saved text (.txt) file with the list of computer names where to deploy agents.
Export	Export the defined list of computers and save it for future use.



Only include single computer names per line in the import file.

3. Click **OK**, once the rule is defined to save and continue with **Deploy Agents** wizard.

2.3 Configuring Agents

2.3.1 Agents settings

To configure additional agents' settings:

1. From **Configuration** tab, select **Agents Management**.
2. Click **Agents Settings**.
3. (Optional) Table 4 below describes the available agent settings:

Table 4 -Agents settings

OPTION	DESCRIPTION
Auto uninstall	Set the number of days after which GFI LanGuard Agents automatically uninstall themselves if the host computer is unresponsive for the set period of days.
Agents report using	Specify the communication ports used by GFI LanGuard and GFI LanGuard Agents.

4. Click **OK** to save and close dialog.



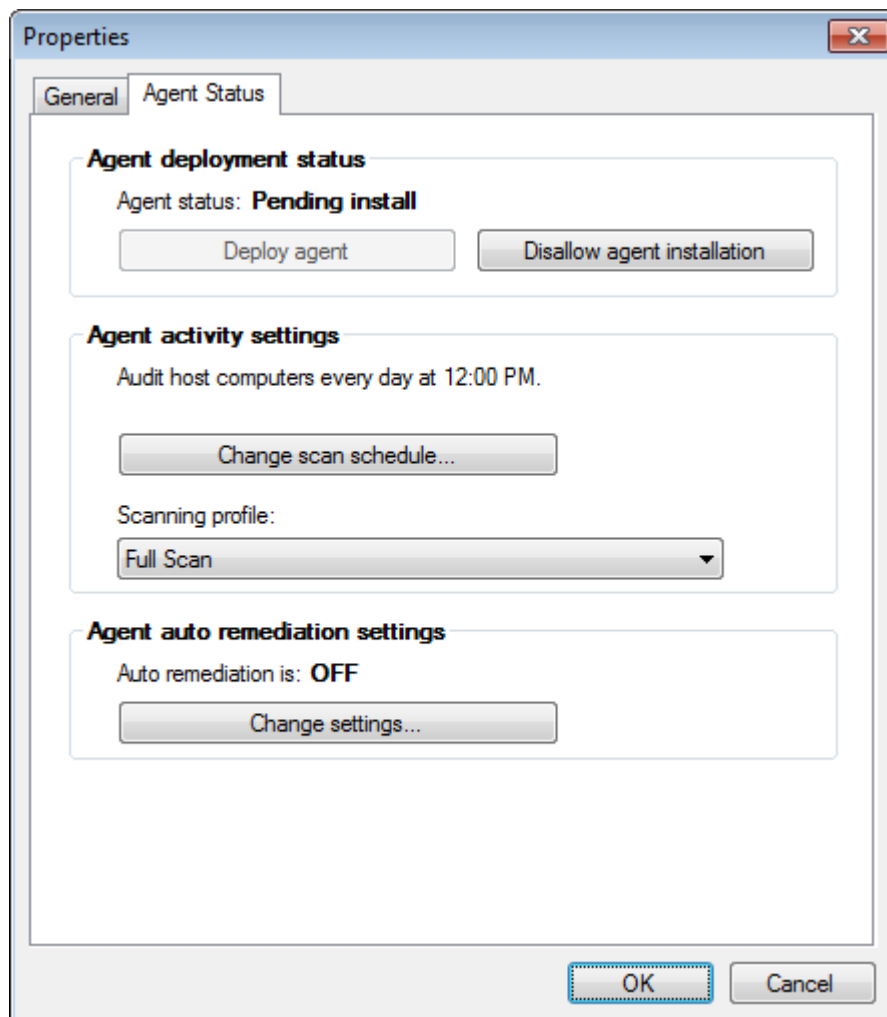
Communication on TCP port 135 and 1070 must be enabled in Windows firewall for GFI LanGuard Agents to send data to GFI LanGuard.

2.3.2 Customizing agents

Agents can be modified through the **Properties** dialog.

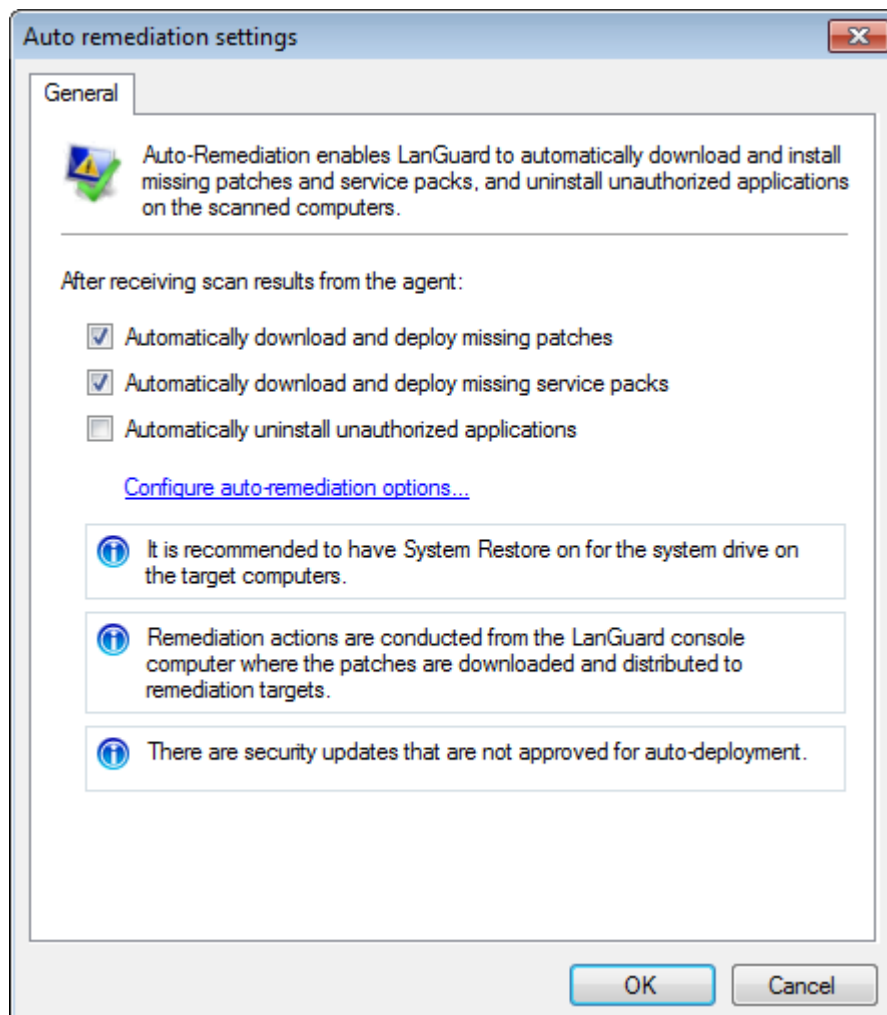
To access agent properties:

1. Click **Configuration** tab ► **Agents Management**.
2. From the right pane, right-click an agent and select **Properties**.
3. (Optional) From **General** tab, specify the authentication method.



Screenshot 5 - Agent properties

4. From **Agent Status** tab, enable/disable agent deployment by clicking **Deploy agent** or **Disallow agent installation**.
5. Click **Change scan schedule...** to configure agent scan schedule and from **Scanning profile**, select the active scan profile.
6. Enable/disable agent auto-remediation. Click **Change settings...** to open **Auto-remediation settings** dialog for that specific agent.



Screenshot 6 - Agent auto-remediation

7. Select **Automatically download and deploy missing patches** to enable automatic remediation for missing patches.
8. Select **Automatically download and deploy missing service packs** to enable automatic remediation for missing service packs.
9. Select **Automatically uninstall unauthorized applications** to enable automatic remediation for unauthorized applications.
10. (Optional) Click **Configure auto-remediation options...** to further customize remediation options.



For information about auto-remediation options, refer to [Auto-remediation options](#) section in this manual.



For information about unauthorized applications, refer to [Automatically uninstall unauthorized applications](#) section in this manual.

3 Agent-less Auditing

3.1 Introduction

Agent-less auditing is the process of performing audits on target computers without using agents. Two types of audits can be done using this approach:

- » **Manual audits** - Perform audits on target computer(s) once.
- » **Scheduled audits** - Perform audits on a target computer(s) repeatedly on a schedule.

On completion of an agent-less audit, GFI LanGuard enables you to analyze the audit results. This section provides information on how to configure manual audits, scheduled audits and analyze the results. For more information on how to analyze results, refer to [Audit Result Summary](#) and [Audit Result Details](#) sections in this manual.

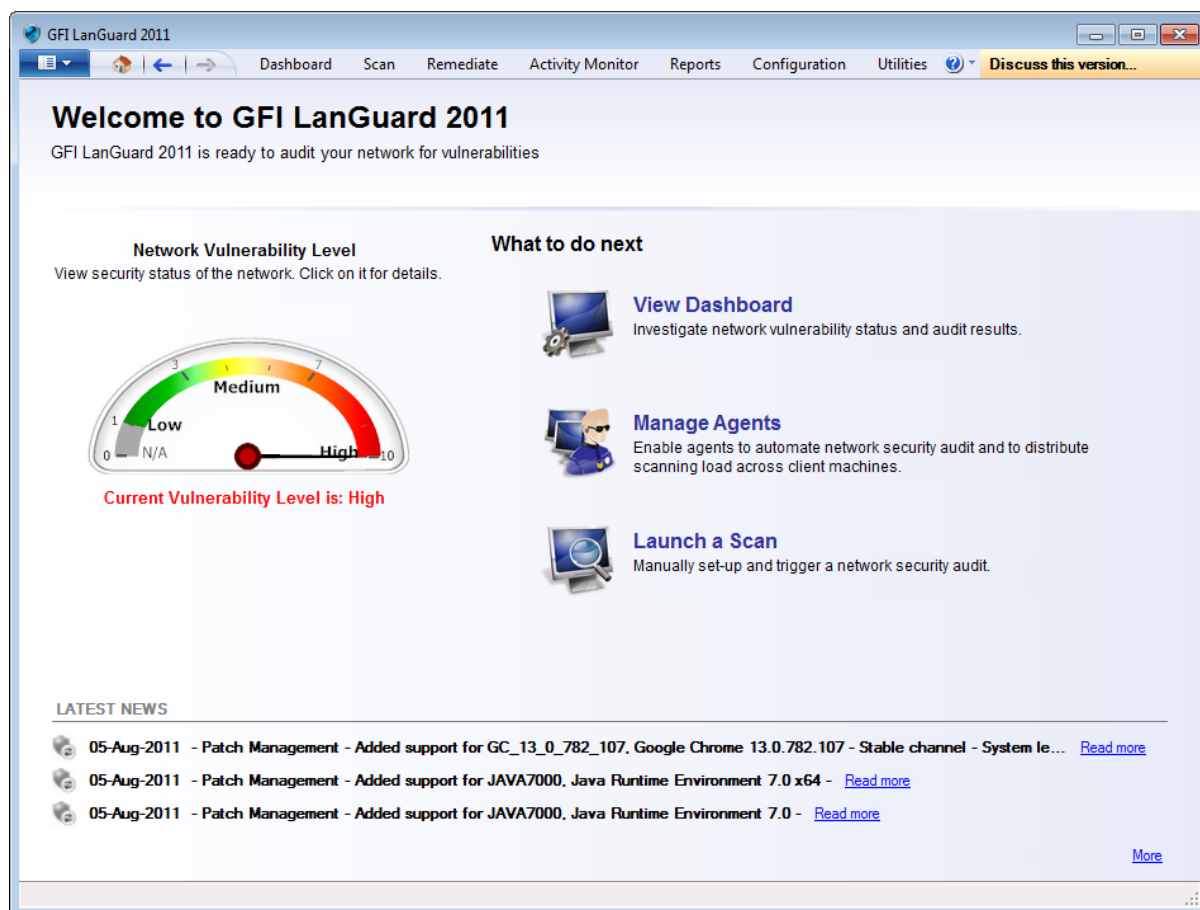
3.2 Performing a manual audit

An effective audit can be done in three steps such as:

- » **Configure scan properties** - configure scan targets and any relative properties required to scan the networked computers.
- » **Analyze scan results** - identify the main network vulnerabilities discovered and the scan targets that require immediate attention.
- » **Remediate vulnerabilities** - implement patches, service packs or fixes to the scanned targets.

3.2.1 Step 1: Configure target properties

1. Launch GFI LanGuard from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.



Screenshot 7 - Launch manual scan

2. From the Home page, select **Launch a scan**.

Launch a New Scan	
Scan Target:	Profile:
file:customgroup_2011_8_4_18_29_59.txt	Full Scan
Credentials:	Username: Password:
Currently logged on user	sa
☒ Use per computer credentials when available	☒ Remember credentials
Scan	

Screenshot 8 - Manual scan settings

3. From the **Scan Target** drop-down menu, select the target computer or group of computers to scan. Table 5 below describes the available options:

Table 5 - Target options when auditing

OPTION	DESCRIPTION
Local host	Audit the local host where GFI LanGuard is installed.
Domain: primary domain	Audit the entire domain / workgroup of the computer / server where GFI LanGuard is installed. For information on how to define custom target properties, refer to the Custom target properties section in this manual.
File	Audit computers specified in a saved text (.txt) file. For information on how to define custom target properties, refer to the Custom target properties section in this manual.

4. From the **Profile** drop-down menu, select the scan profile that you want GFI LanGuard to action during the scan.
5. From the **Credentials** drop-down menu, select the log-on method used by GFI LanGuard to log onto the scan targets.

Table 6 below describes the available log-on methods:

Table 6 - Logon and audit options

OPTION	DESCRIPTION
Currently logged on user	Use the current logged on user credentials when logging on scan targets.
Alternative credentials	Use custom credentials. Key-in the user name and password to use.
A null session	Log onto scan targets using a null session. The user will log onto the target machine as an anonymous user.
A private key file	Log onto UNIX machines using SSH. A user name and password is required.

6. (Optional) Select **Use per computer credentials when available** to logon target machines using the credentials specified in the Dashboard. For more information on how to configure computer credentials using the dashboard, refer to [Configure credentials](#) section in this manual.
7. (Optional) Select **Remember credentials** to use the configured credentials as default when performing an audit.
8. Click **Scan** to start auditing the selected targets.



For more information on Scanning Profiles, refer to the [Scanning Profiles](#) section in this manual.



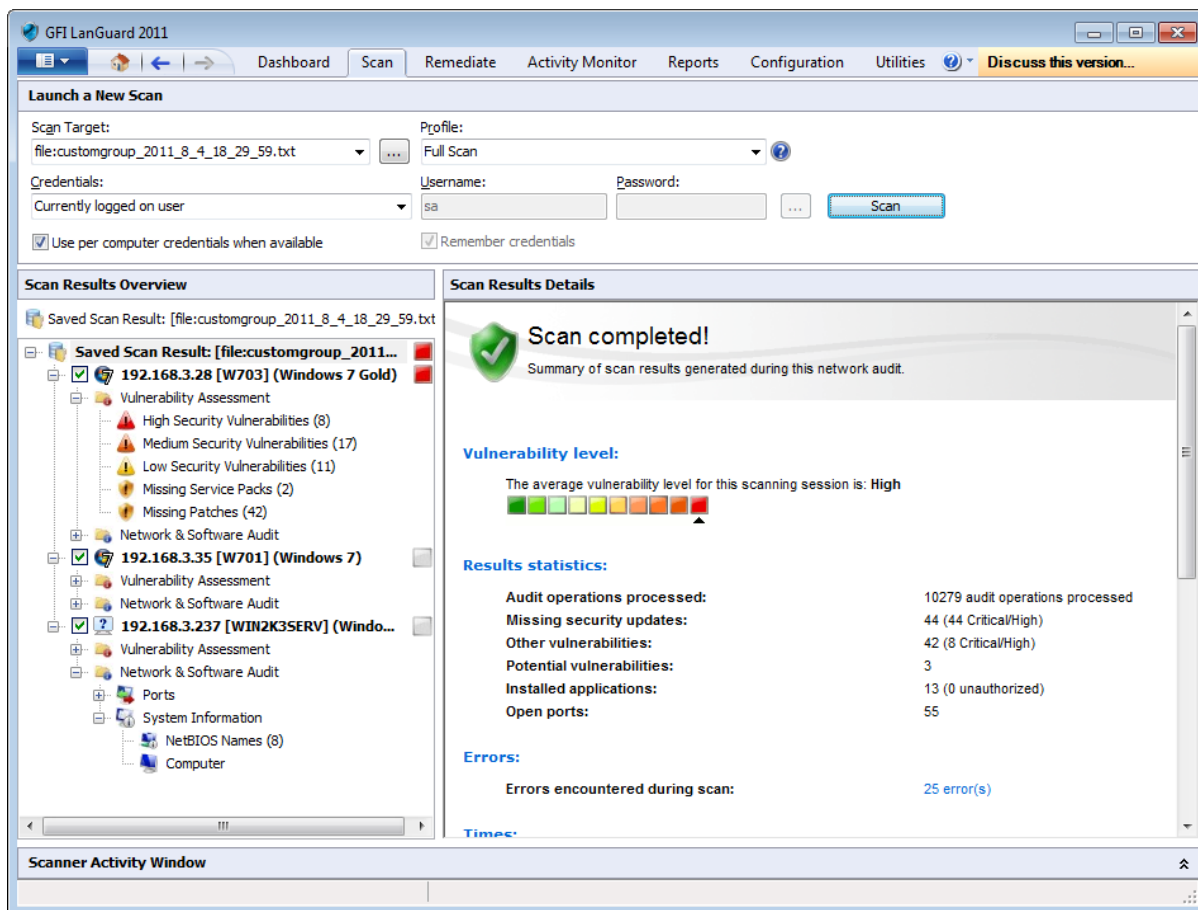
The credentials provided need to have administrator privileges in order for GFI LanGuard to log-on to the target computers and carry out the network audit.

3.2.2 Step 2: Analyze scan results

One of the key steps in a network security audit is to analyze scan results and identify the most vulnerable areas that require immediate attention. The **Scan Results Overview** and **Scan Results Details** sections provide this information.

To analyze scan results:

1. Launch GFI LanGuard from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Launch a scan or load a scan from a saved file.



Screenshot 9 - Scan result details

3. From the **Scan** tab, analyze the scan results from the provided views described below:

Table 7 - Scan Results

SECTION	DESCRIPTION
Scan Results Overview	Provides summarized information about the last scan. Information provided includes: » Scanned target names » The number and type of vulnerabilities detected during the scan.
Scan Results Details	This section enables users to select a scan target from the Scan Results Overview section in order to display detailed information about every vulnerability detected on the selected computer.



For more information about scan results, refer to [Audit Result Summary](#), [Audit Result Details](#) and [Analyzing Results](#) sections in this manual.



To load saved scan results, go to **File ► Load Scan Results from ► Database/XML file**.

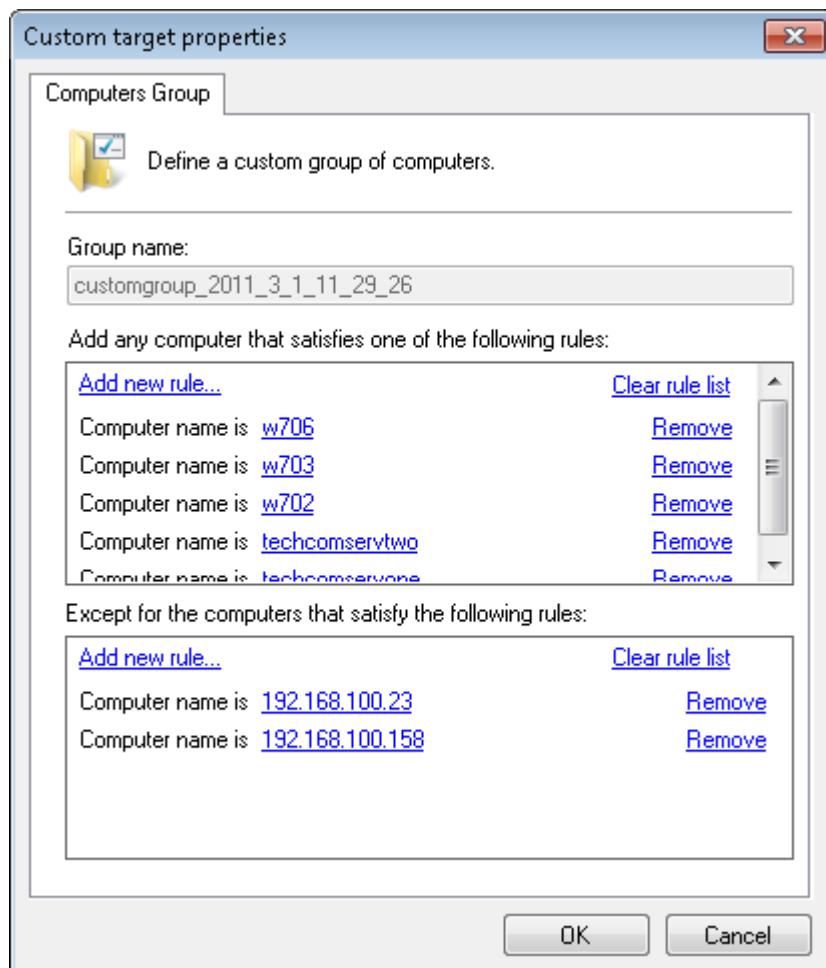
3.2.3 Step 3: Remediate vulnerabilities

GFI LanGuard enables you to immediately remediate the detected vulnerabilities through the **Remediate** tab. For more information on remediating vulnerabilities, refer to [Fixing Vulnerabilities](#) section in this manual.

3.2.4 Custom target properties

Target rules are custom rules used by GFI LanGuard to find a target computer or a domain.

Click **Scan** tab ► ... (define button), to launch **Custom target properties** dialog.



Screenshot 10 - Custom target properties

To create a new target rule:

1. Click **Add new rule...** and configure search criteria. Table 8 below describes the available rule types:

Table 8 - Custom target properties

RULE TYPE	DESCRIPTION
Computer name is	Search and add computers by name. Key-in a valid computer name and click Add for each computer. Click OK to apply changes.
Computers file list is	Search and add computers from a text file. Click the browse button and locate the text file. Click OK to apply changes. NOTE: When submitting a list of target computers from file, ensure that the file contains only one target computer name per line.
Domain name is	Search and add computers that are members of a domain. Select the domains from the list and click OK .
IP address is	Search and add computers by IP address. Select This computer to add the local host or Scan another computer to add a remote computer. Key-in the IP address if required and click OK .

RULE TYPE	DESCRIPTION
IP address range is	Search and add computers within an IP range. Select Scan an IP address range and key in the IP range or select CIDR subnet and key-in the range using CIDR notation. NOTE: The Classless Inter-Domain Routing (CIDR) provides an alternative way of specifying an IP address range. The notation is as follows: <Base address> / <IP network prefix>. Example: 192.168.0.0/16
Organization unit is	Search and add computers within an organizational unit. Click Select and from the list select the Organizational units. Click OK .

2. To identify the rule for future use key-in a valid name in **Group name** and click **OK**.

3.3 Scheduled scan

A scheduled scan is a network audit that is scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically. Scheduled scan status is monitored using the **Activity Monitor** tab ► **Security Scans**.

Scheduled scans also enable:

- » Automatic download and deployment of missing updates detected during a scheduled audit.
- » Email notifications on network threats detection.
- » Consecutive scan comparison reports generation and email distribution.
- » Automatic uninstallation of unauthorized applications.

3.3.1 When to use scheduled Scans?

GFI recommends scheduled scans:

- » When GFI LanGuard Agent is not deployed on the target computer.
- » To automatically perform periodical/regular network vulnerability scans using same scanning profiles and parameters
- » To automatically trigger scans after office hours and generate alerts and auto-distribution of scan results via email.
- » To automatically trigger auto-remediation options, (Example: Auto download and deploy missing updates).



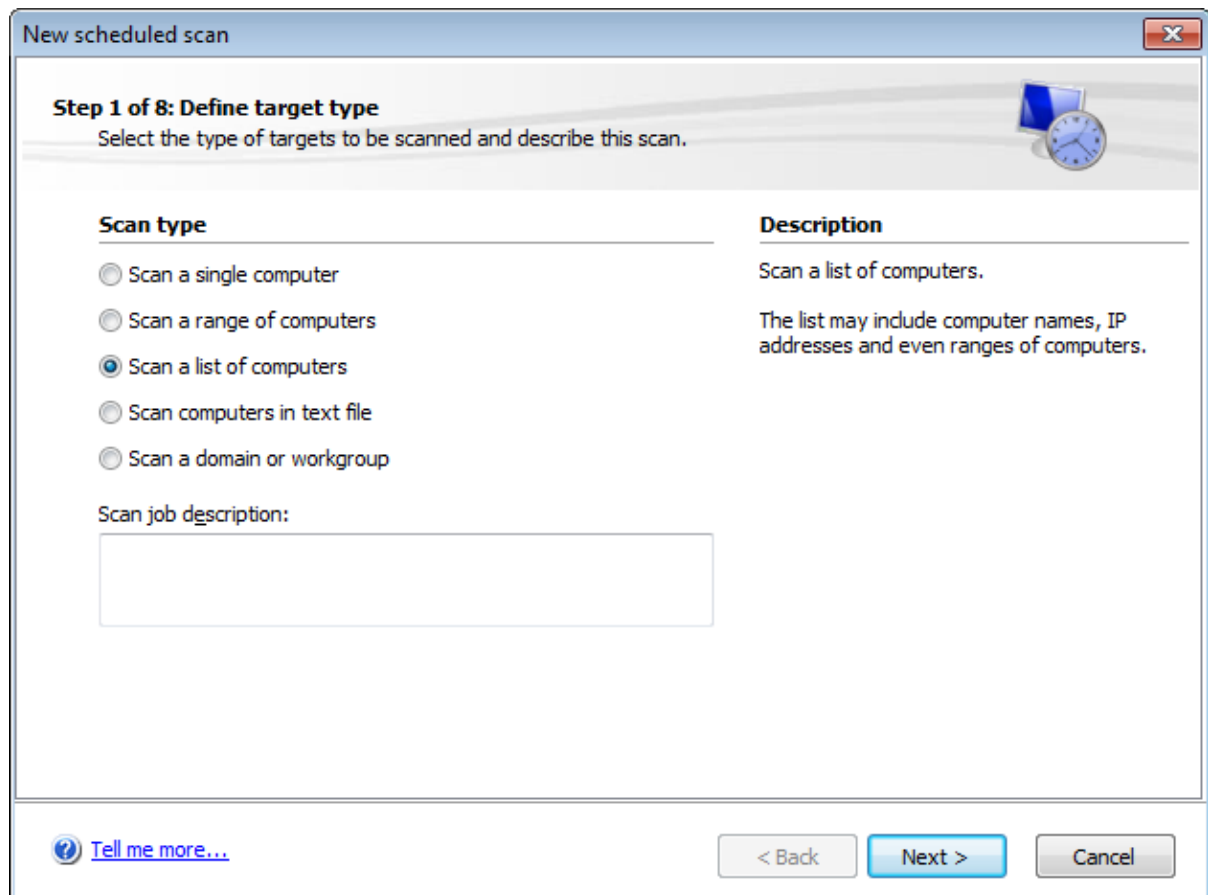
For more information on auto-remediation and deployment, options refer to **Automatic Remediation** section in this chapter



Ensure that the GFI LanGuard Attendant service is running otherwise scheduled operations will fail to start. To view GFI LanGuard Attendant service, click **Start ► Run**, key-in **services.msc** and press **Enter**. Locate GFI LanGuard Attendant Service and ensure that Status is **Started**.

3.4 Setting up scheduled scans

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Configuration** tab ► **Scheduled Scans**.
3. From **Common Tasks**, select **New scheduled scan...**



New scheduled scan

Step 1 of 8: Define target type
Select the type of targets to be scanned and describe this scan.

Scan type

- ☐ Scan a single computer
- ☐ Scan a range of computers
- ☒ Scan a list of computers
- ☐ Scan computers in text file
- ☐ Scan a domain or workgroup

Description

Scan a list of computers.
The list may include computer names, IP addresses and even ranges of computers.

Scan job description:

[Tell me more...](#) < Back Next > Cancel

Screenshot 11 - New Scheduled Scan dialog

4. Select one of the options described in Table 9 below and click **Next**:

Table 9 - New scheduled scan type

OPTION	DESCRIPTION
Scan a single computer	Scan local host or one specific computer.
Scan a range of computers	Scan a number of computers defined through an IP range. For more information refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002749
Scan a list of computers	Manually create a list of targets, import targets from file or select targets from network list.
Scan computers in text file	Scan targets enumerated in a specific text file.
Scan a domain or workgroup	Scan all targets connected to a domain/workgroup.

5. Depending on the option selected in the previous step, specify the respective target computer(s) details and click **Next**.

New scheduled scan

Step 3 of 8: Set the triggering time
Set the triggering time for this scheduled scan job.

Triggering time

☐ One time only, on: 04/08/2011 at: 18:19:39
☒ Recurrence pattern: daily at: 18:19:39
☒ Every 1 days
☐ Every weekday

☒ Wait for offline machines to connect to the network.

Description
Set the triggering time for this scheduled scan job

 If nonexistent systems are specified in the scan target the scan will not finish until the user manually stops it from Activity Monitor -> Security Scans.

[Tell me more...](#) < Back Next > Cancel

Screenshot 12 - Scheduled scan frequency

6. Specify date/time/frequency of scheduled scan and click **Next**.

New scheduled scan

Step 4 of 8: Select scan profile
Select parameters to use for scan job.

Scan profile

Scan job operation:
Network & Software audit

Select scan profile:

- Full TCP & UDP Scan
- Only SNMP
- Ping Them All
- Share Finder
- Uptimes
- Disks Space Usage
- System Information
- Hardware Audit
- Network Discovery

Description
Discover open TCP/UDP ports commonly exploited by Trojans.

NOTE: Scan profiles contain pre-set parameters used by the scanner for the job type selected.

[Tell me more...](#) < Back Next > Cancel

Screenshot 13 - Select scanning profile

7. Specify the scanning profile and click **Next**.

New scheduled scan

Step 5 of 8: Remote logon credentials
Specify credentials to use to log on to remote targets.

Credentials	Description
☐ GFI LanGuard 10 Attendant Service account	Use data from computer profiles
☒ Alternative credentials	
User name: Administrator	
Password:	
☐ SSH Private Key	
User name:	
Key file:	...

☒ Use per computer credentials when available

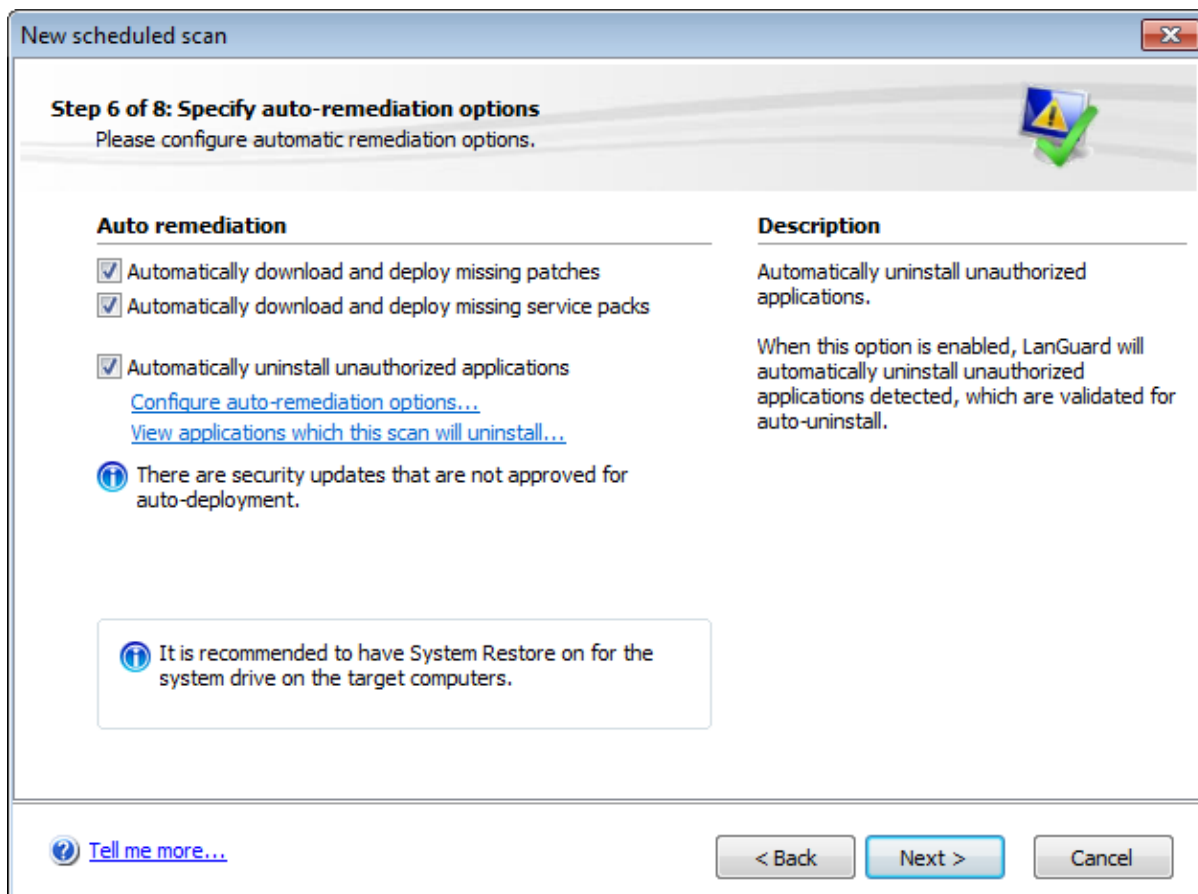
[? Tell me more...](#) < Back Next > Cancel

Screenshot 14 - Remote logon credentials

8. (Optional) Specify **Remote logon credentials** and click **Next**. Remote logon credentials can be either one of the following:

Table 10 - Remote logon credentials

OPTION	DESCRIPTION
GFI LanGuard 10 Attendant Service account	Performs the scan using the credentials specified while installing GFI LanGuard 2011.
Alternative credentials	Specify alternate credentials to connect to the scan computers. NOTE: Ensure the supplied credentials have administrative privileges.
SSH Private Key	Key in a username and select the key file used to logon to UNIX/LINUX based systems.
Use per computer credentials when available	Use predefined credentials for the scan being configured. For more information, refer to Configure credentials section in this manual.



Screenshot 15 - Scheduled scan auto-remediation options

9. From the auto-remediation dialog, select the required options and click **Next**. Table 11 below describes the list of available options:

Table 11 - Auto-remediation options

OPTION	DESCRIPTION
Automatically download and deploy missing patches	Automatically download and deploy missing patches on target machines.
Automatically download and deploy missing service packs	Automatically download and deploy missing service packs on target machines.
Automatically uninstall unauthorized applications	If this option is selected all applications validated as unauthorized, will be uninstalled from the scanned computer (unauthorized applications are defined in Application Inventory). For more details see Application auto-uninstall
Configure auto-remediation	Automatically remove unauthorized applications from target machines. Unauthorized applications are defined in the Application Inventory). For more details see Application auto-uninstall
View applications which this scan will uninstall	Click the link to launch the Applications which will be uninstalled dialog. This will list all the applications that will be uninstalled when the scheduled scan is finished.

New scheduled scan

Step 7 of 8: Configure reporting options
Choose which reporting options you would like to enable for this scheduled scan.

Reporting options	Description
☒ Email the scan report	You may enable emailing and/or saving of the scan reports and choose the data to include in the report.
☐ Save the scan report to disk: C:\ProgramData\GFI\LanGuard 10\Reports	
Choose scan report content:	
☒ Comparison data and auto remediation details	
☐ Full scan results data	
Configure alerting options... Alerting options are not configured!	
Scans for large networks will generate a large report!	

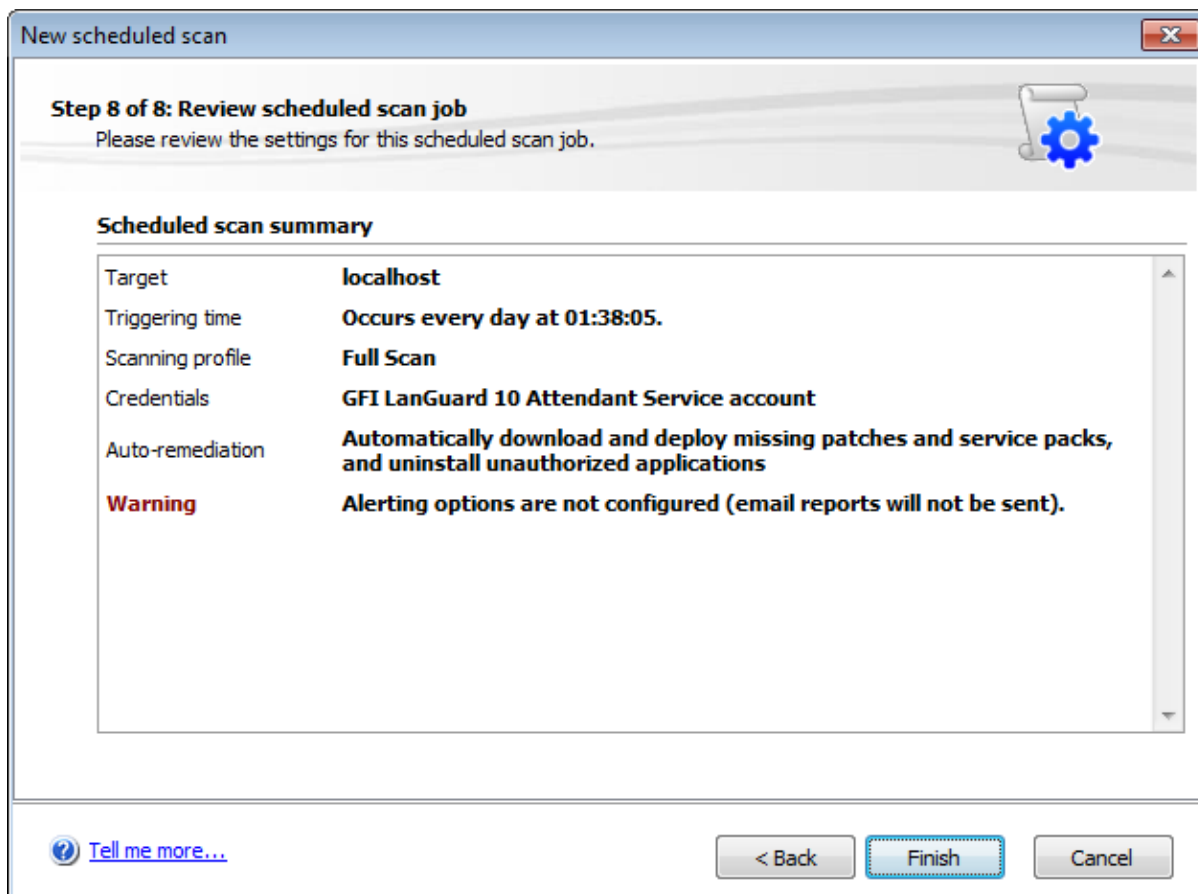
[Tell me more...](#) < Back Next > Cancel

Screenshot 16 - Scheduled scan reporting options

10. (Optional) Configure **Reporting options** as described below:

Table 12 - Reporting options

OPTION	DESCRIPTION
Email the scan report	Send a report by email at the end of each scheduled scan.
Save the scan report to disk	Save a report to disk at the end of each scheduled scan.
Comparison data and auto remediation details	Include details of auto remediation actions performed and result comparison with previous security scans. NOTE: Comparison is done between scans with same scan target(s) and scanning profile.
Full scan results data	Include full scan result details.
Configure alerting options	(Optional) Click Configure alerting options... to specify sender/recipient details. For information on configuring alerting options, refer to Configuring alerting options section in this manual.

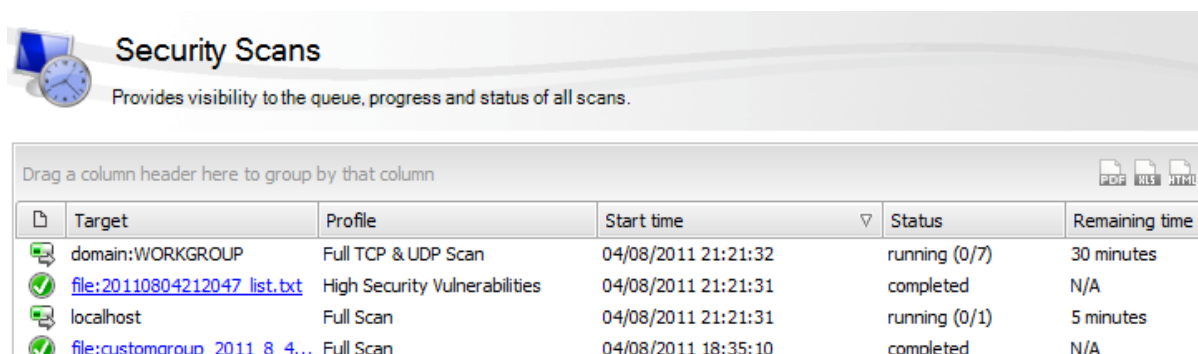


Screenshot 17 - Review scheduled scan job

13. Click OK and Finish.

By default, all new scheduled scans are disabled. To enable, select **Configuration** tab ► **Scheduled Scans** and click on the button.

Confirm that the new scheduled scans are successfully set by clicking on **Activity Monitor** tab ► **Security Scans**. New scheduled scans are listed in the queue.



Screenshot 18 - Scheduled scan status



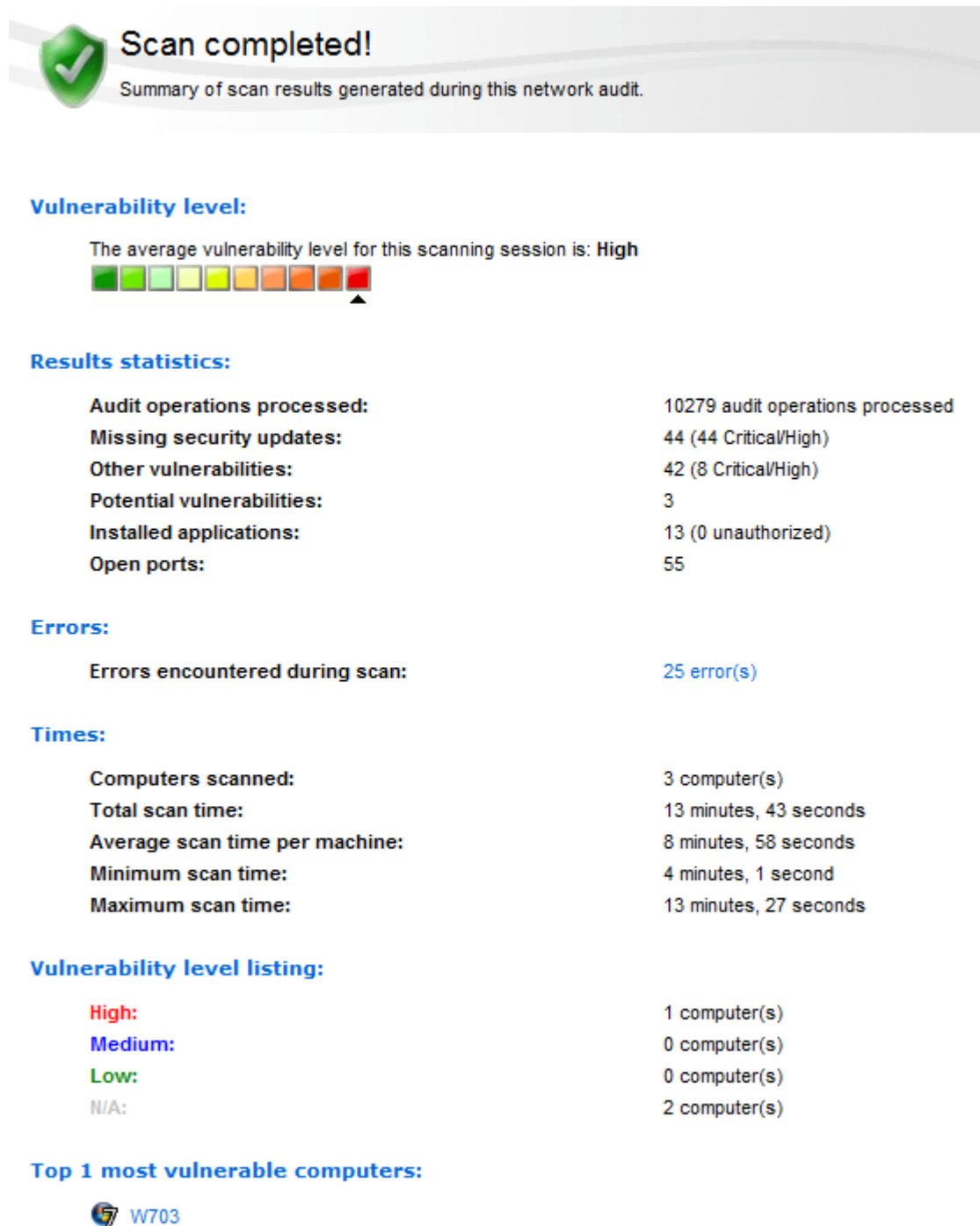
For more information on Scheduled Scans refer to the [Scheduled Scans](#) section in this manual.

3.5 Audit result summary

On completion of a network security scan, it is important to identify the areas that require immediate attention. The correct analysis and interpretation of information collected enables you to achieve this goal.

To view the progress and results of an audit:

1. Wait for a scan to complete or load a result from the database/file. For more information on how to load results from the database, refer to [Loading saved scan results from database](#) section in this manual.
2. Click **Scan**.



Screenshot 19 - Scan summary

3.5.1 Vulnerability level rating

The vulnerability level is a rating given by GFI LanGuard to each computer after it is scanned. The rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found.

Vulnerability level:

The average vulnerability level for this scanning session is: **High**



Screenshot 20 - Vulnerability level meter

High vulnerability ratings are the result of identified vulnerabilities and /or missing patches that are classified as high risk.

When a number of computers are scanned in a single audit session, a measurement of the global vulnerability level is based on a weighted sum of the vulnerabilities detected on the computers scanned.

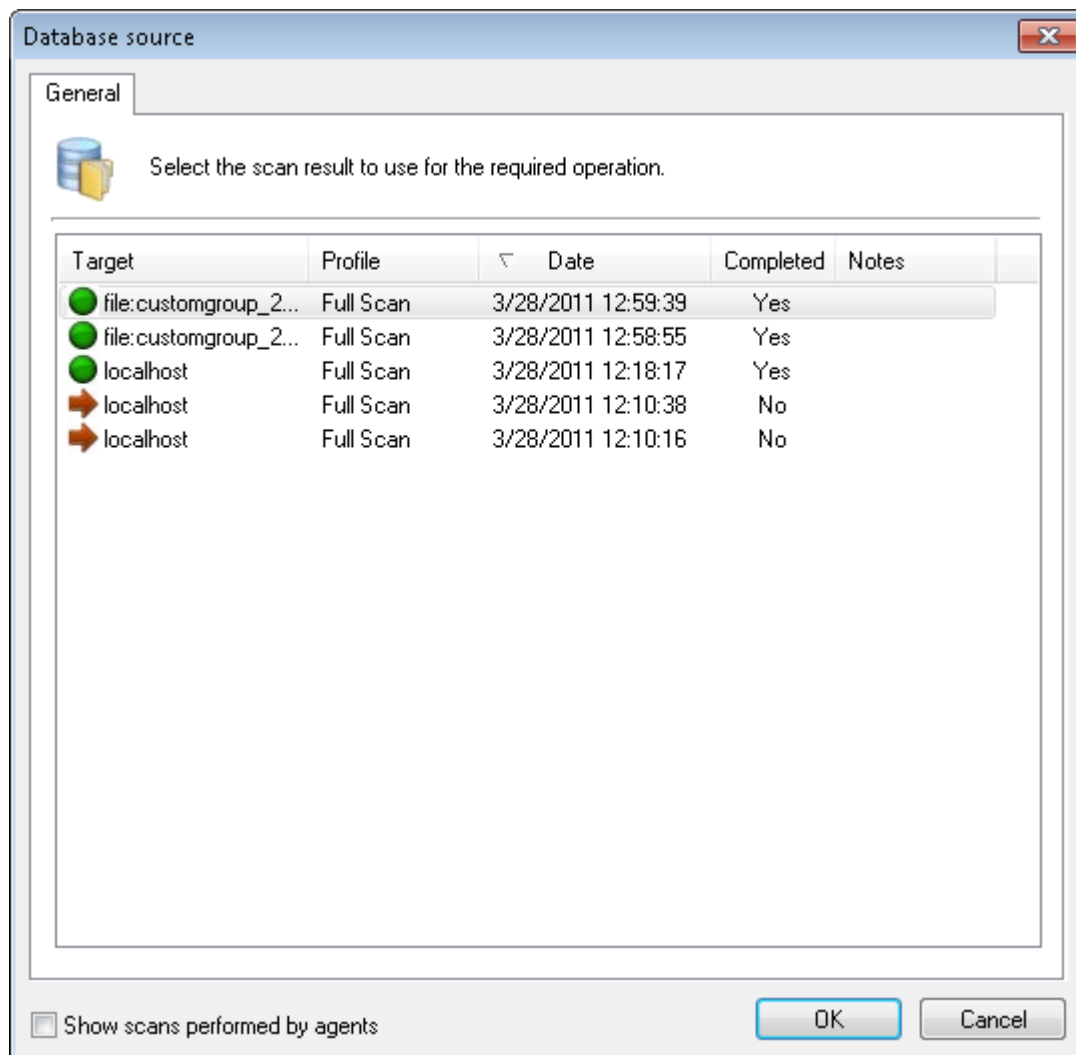
The Vulnerability level is indicated using color-coded graphical bar. A red colour-code indicates a high vulnerability level, while a green colour-code indicates a low vulnerability level.

3.5.2 Loading saved scan results from database

By default, saved scan results are stored in a database. GFI LanGuard stores the results data of the last 10 scans performed per scanning profile. You can configure the number of scan results that are stored in a database file. For more information, refer to the [Database maintenance options](#) section in this manual.

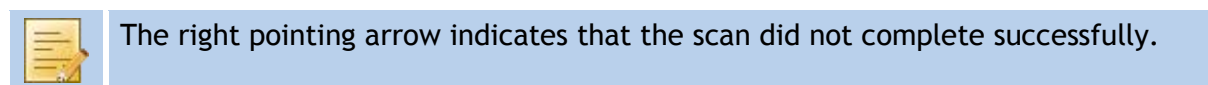
To load saved scan results from the database backend or from XML files:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click the **GFI LanGuard** button ► **File ► Load Scan Results from ► Database...**



Screenshot 21 - Reloaded scan results

3. Select the saved scan result and click **OK**.



3.5.3 Save and load scan result in XML format

Scan results are an invaluable source of information for systems administrators. GFI LanGuard results are stored in a Microsoft-SQL Server or a Microsoft-Access database. In addition, scan results can also be exported to XML.

To save scan results to XML file:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click on **Scan**.
3. Launch a new scan or load a scan from the database.
4. Click the **GFI LanGuard** button ► **File ► Save Scan Results**.
5. Locate the destination where you want to save the XML and click **Save**.

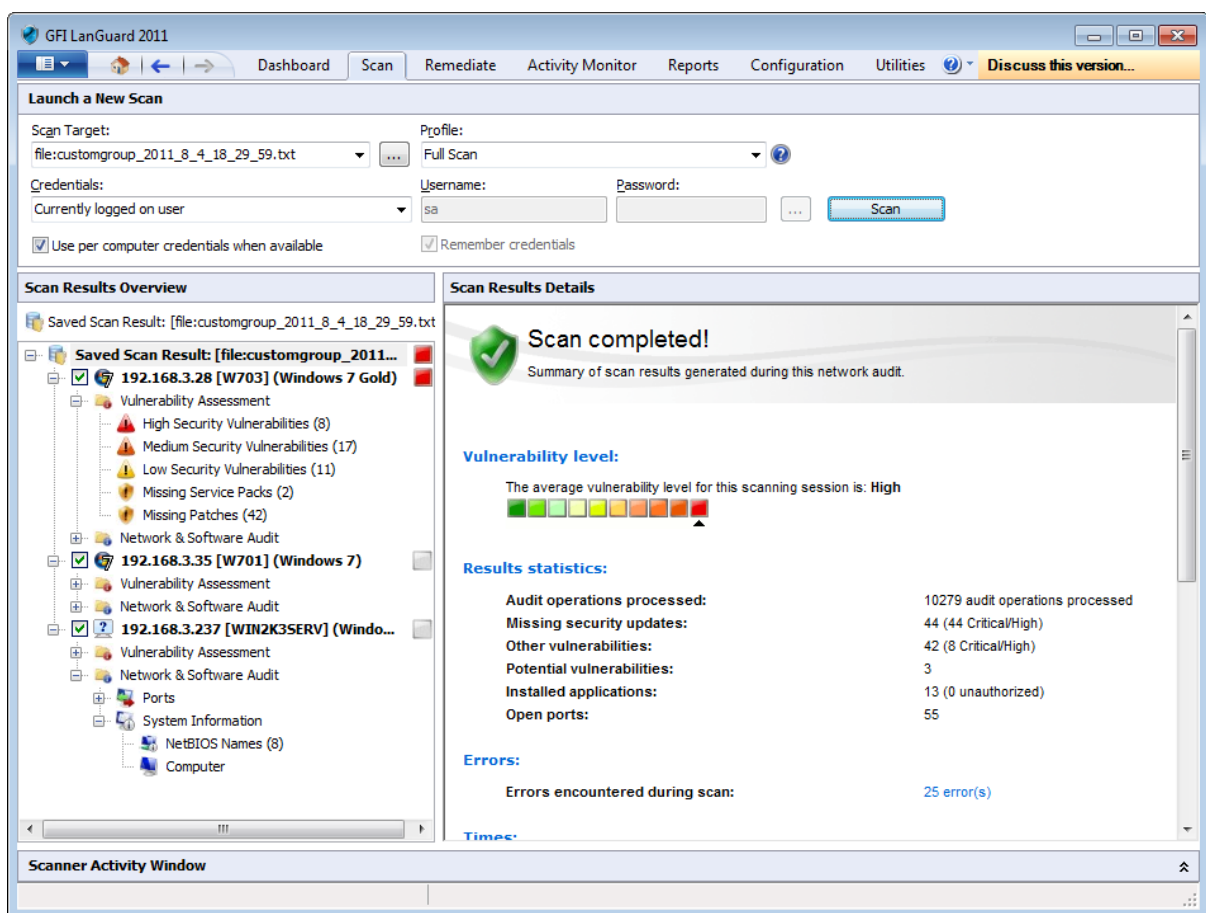
To load saved scan results from an XML file:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click the **GFI LanGuard** button ► **File ► Load Scan Results from ► XML File...**
3. Locate the scan results to load and click **OK**.

3.6 Audit result details

On scan completion, the **Results** section displays a graphical representation of the vulnerability level including the scan result in more detail. To access the Results section:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Wait for a scan to complete or load a result from the database/file.
3. Click **Scan**.



Screenshot 22 - Detailed view tab

Scan Results Overview	Displays information related to the scanned computer or domain.
Scan Results Details	Displays information related to the scan performed on target computer including vulnerabilities found, system patching status, etc.

From **Scan Results Overview**, expand a computer node to access results retrieved during the scan. Security scan results are organized in two sub-nodes tagged as:

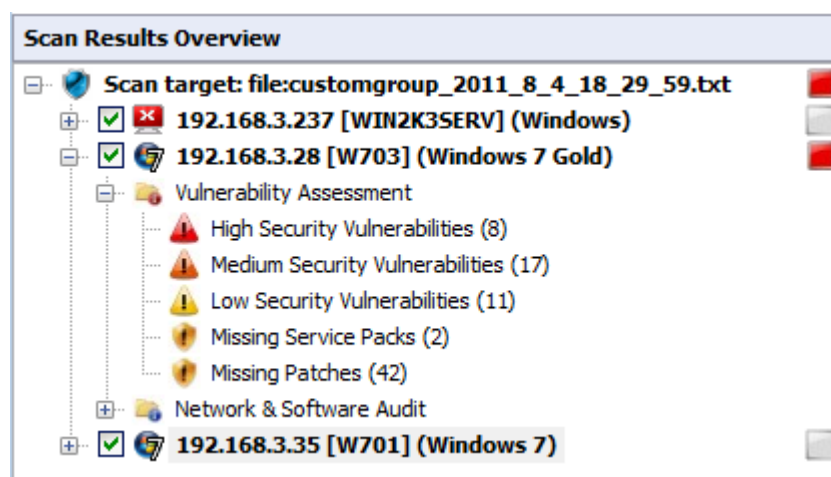
- » **Vulnerability Assessment**
- » **Network & Software Audit**

While a scan is in progress, each computer node has an icon that categorizes the response time. Table 13 below describes the different icons used by GFI LanGuard to categorize the response time. The first icon indicates that the scan is queued, while the second icon indicates that the scan is in progress.

Table 13 - Response time icons

CATEGORY	INFORMATION	RESPONSE TIME IN MILLISECONDS
 	Fast response	Less than 25ms
 	Medium response	Between 25ms and 100ms
 	Slow response	More than 100ms

3.6.1 Vulnerability assessment



Screenshot 23 - The Vulnerability Assessment node

Click on any **Vulnerability Assessment** node to view the security vulnerabilities identified on the target computer grouped by type and severity as follows:

- » **High Security Vulnerabilities**
- » **Low Security Vulnerabilities**
- » **Potential vulnerabilities**
- » **Missing Service Packs**
- » **Missing Patches**

High/Med/Low Security vulnerabilities

Click on the  **High Security Vulnerabilities** or  **Low Security Vulnerabilities** sub-nodes for a list of weaknesses discovered while auditing a target device. Table 14 below describes these groups:

Table 14 - GFI LanGuard Vulnerability groups

GROUP	DESCRIPTION
Mail, FTP, RPC, DNS and Miscellaneous	Shows vulnerabilities discovered on FTP servers, DNS servers, and SMTP/POP3/IMAP mail servers. Links to Microsoft Knowledge Base articles or other support documentation are provided.

GROUP	DESCRIPTION
Web	Lists discovered vulnerabilities on web servers (such as wrong configuration issues). Supported web servers include Apache, Netscape, and Microsoft I.I.S.
Services	Lists vulnerabilities discovered in active services as well as the list of unused accounts that are still active and accessible on scanned targets.
Registry	Registry settings of a scanned network device are listed. Links to support documentation and short vulnerability descriptions are provided.
Software	Enumerates software installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.
Rootkit	Enumerates discovered vulnerabilities because of having a rootkit installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.

Potential vulnerabilities

Select  **Potential vulnerabilities** sub-node to view scan result items classified as possible network weaknesses. Although not classified as vulnerabilities, these scan result entries still require particular attention since malicious users can exploit them during malicious activity.

For example, during vulnerability scanning GFI LanGuard enumerates all modems installed and configured on target computers. If unused, modems are of no threat to your network. If connected to a telephone line these modems can however be used to gain unauthorized and unmonitored access to the Internet. Users can potentially bypass corporate perimeter security including firewalls, anti-virus, website rating and web content blocking. This exposes the corporate IT infrastructure to a wide range of threats including hacker attacks. GFI LanGuard considers installed modems as possible threats and enumerates them in the **Potential Vulnerabilities** sub-node.

Missing Service Packs/Patches

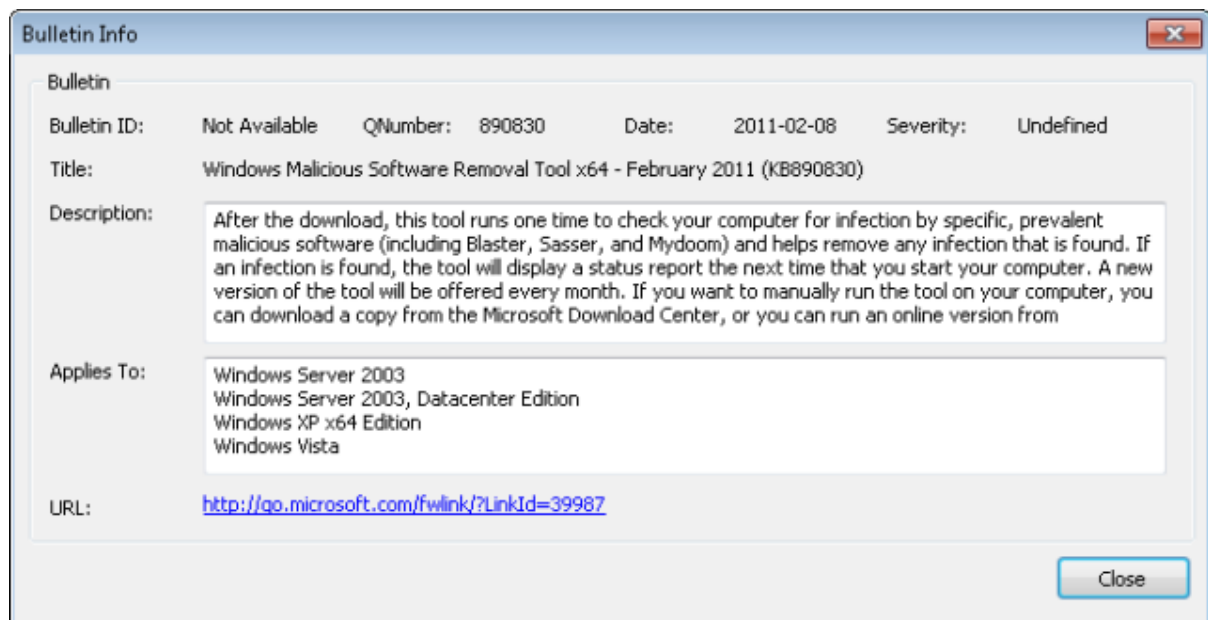
Click  **Missing Service Packs** or  **Missing Patches** sub-node to check any missing software updates or patches.



GFI LanGuard can identify missing service packs and patches on various products. For a complete list of supported products visit:
<http://kbase.gfi.com/showarticle.asp?id=KBID002573>

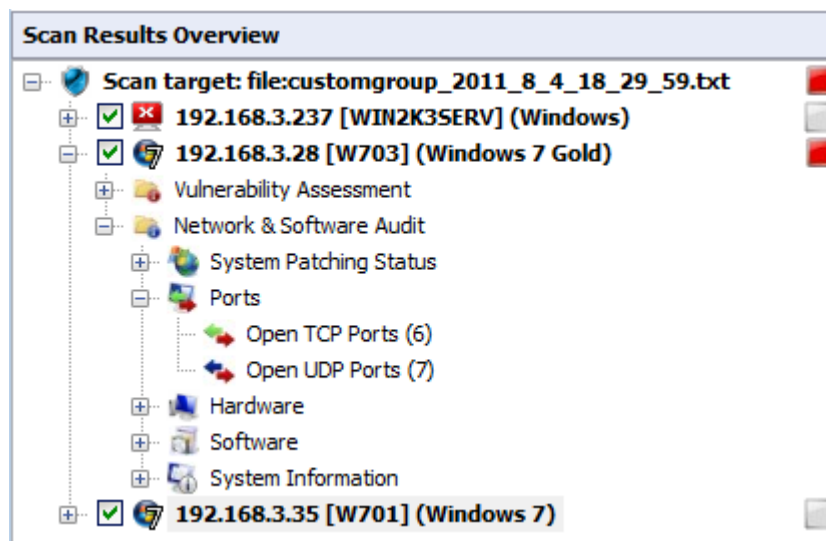
Bulletin information

To access bulletin information, right-click on the respective service pack and select **More details ► Bulletin Info**.



Screenshot 24 - Missing Service pack: Bulletin info dialog

3.6.2 Network & Software Audit



Screenshot 25 - The network and software audit node

Click **Network & Software Audit** to view security vulnerabilities identified on scanned targets. Here, vulnerabilities are grouped by type and severity as follows:

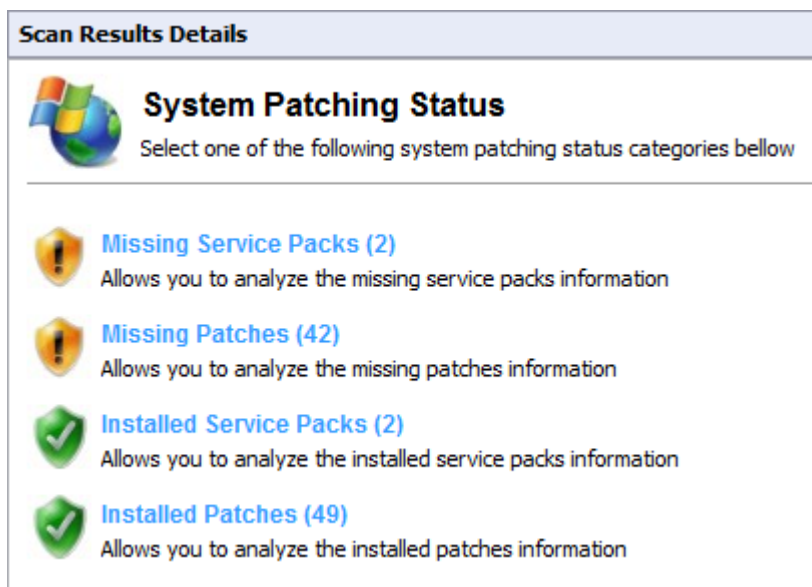
- » System Patching Status
- » Ports
- » Hardware
- » Software
- » System Information

System Patching Status

Click **System Patching Status** to view all missing and installed patches on a target machine.

Table 15 - System patching status

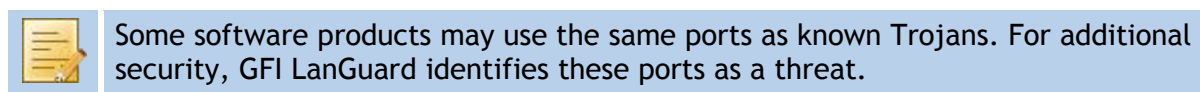
ICON	DESCRIPTION
Missing Patches	Missing software patches.
Installed Service Packs	Installed service packs.
Installed Patches	Installed software patches



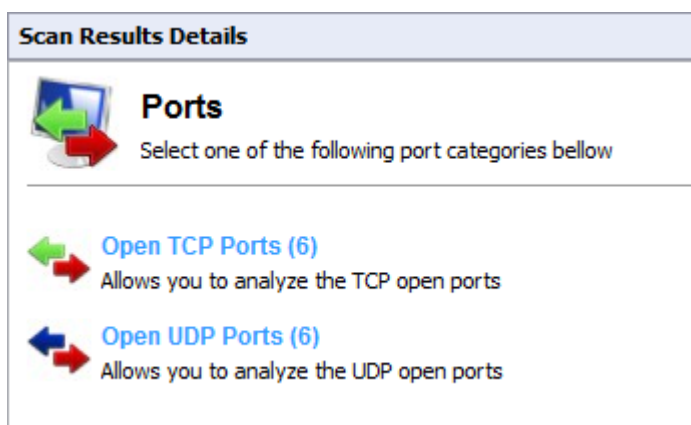
Screenshot 26 - System patches status

Ports

Click **Ports** to view all open TCP and UDP ports detected during a scan. If a commonly exploited port is discovered to be open, GFI LanGuard marks it in red.



Apart from detecting open ports, GFI LanGuard uses service fingerprint technology to analyze the service(s) that are running behind the detected open port(s). With service fingerprint, GFI LanGuard can detect if malicious software is using the detected open port.



Screenshot 27 - All UDP and TCP ports, found during a scan

Hardware

Click **Hardware** to view all details discovered by the hardware audit. The hardware audit, amongst others, displays information such as MAC addresses, IP addresses, device type; device vendor etc. Table 16 below describes the hardware information groups:

Table 16 - Hardware information from an audit

ICON	DESCRIPTION
	Network Devices, including information of all physical, virtual and software-enumerated devices.
	Local Drives, including information on local drives such as available disk space and file system type.
	Processors, including information regarding the processor of a target machine, such as vendor name and processor speed.
	Motherboard, including information regarding the motherboard of a target machine, such as product name, manufacturer, version and serial number.
	Memory details, including information regarding the memory allocation of a target machine, such as free physical/virtual memory available.
	Storage details, including information regarding the storage of a target machine, such as floppy disk drive, CD-ROM and hard drives.
	Display adapters, including information regarding the display and video devices of a target machine, such as the device manufacturer.
	Other devices, including information of devices that does not fall under the mentioned categories above, such as keyboard, ports, mouse and human interface devices.

Software

Click **Software** to view all details involved in the software audit. The software audit amongst others displays information such as:

- » application name
- » publisher
- » version

Table 17 below describes the hardware information groups:

Table 17 -Software information from an audit

ICON	DESCRIPTION
	General Applications - Enumerates installed software on scan targets..
	Antivirus Applications - Lists installed antivirus engines on scan targets.
	Instant Messenger Applications - Lists all detected instances of Instant messenger applications on scan targets.
	Patch Management Applications - Specifies information of installed patches on scan targets.
	Web Browser Applications - Contains scanned targets that have Internet browsers installed.
	Firewall Applications - Enumerates information on installed Firewall applications on scan targets.
	Anti-phishing Applications - Lists information of installed anti-phishing engines on scan targets.

ICON	DESCRIPTION
	VPN Client Applications - Includes information on installed Virtual Private Network clients on scan targets.
	Peer-To-Peer Applications - Shows installed Peer-To-Peer applications on scan targets.

System Information

Click **System Information** to view all details related to the operating system installed on a target machine. Table 18 below describes the system information groups:

Table 18 - System information from an audit

CATEGORY	INFORMATION PROVIDED	HELPS TO IDENTIFY
 Shares	» Share name » Share remark (extra details on the share). » Folder which is being shared on the target computer » Share permissions and access rights » NTFS permissions and access rights.	» Users sharing entire hard-drives, shares that have weak or incorrectly configured access permissions » Startup folders, and similar system files, that are accessible by unauthorized users, or through user accounts, that do not have administrator privileges, but are allowed to execute code on target computers. » Unnecessary or unused shares.
 Password Policy	» Minimum password length » Maximum password length » Minimum password expiry date » Force logoff » Password history.	» Incorrectly configured lockout control » Password strength enforcement policies.
 Security Audit Policy	» Audit account logon events » Audit account management » Audit directory service access » Audit logon events » And more...	» Security holes or breaches.
 Registry	» Registered owner » Registered organization » Product name » Current build number.	» Hardware and software settings such as which drivers and applications will be automatically launched at system startup.
 NETBIOS Names	» Workstation service » Domain name » Domain controllers » File server service.	» Rogue computers » Wrong configurations.
 Computer	» MAC address » Time to live (TTL) » Network role » Domain.	» Rogue computers » Wrong configurations.

CATEGORY	INFORMATION PROVIDED	HELPS TO IDENTIFY
 Groups	» Account operators » Administrators » Backup operations » Guest.	» Wrong configurations » Security flaws due to rogue or obsolete user groups.
 Users	» Full name » Privilege » Flags » Login.	» Rogue, obsolete or default user accounts.
 Logged On Users	» List of logged on users.	» Authorized and unauthorized users currently logged on computers.
 Sessions	» Lists hosts remotely connected to the target computer during scanning.	» Authorized and unauthorized remote connections.
 Services	» List of active services.	» Rogue or malicious processes; redundant services.
 Processes	» List of active processes.	» Rogue or malicious processes.
 Remote TOD (time of day)	» Time of remote workstation, server or laptop.	» Time inconsistencies and regional settings » Wrong configurations.

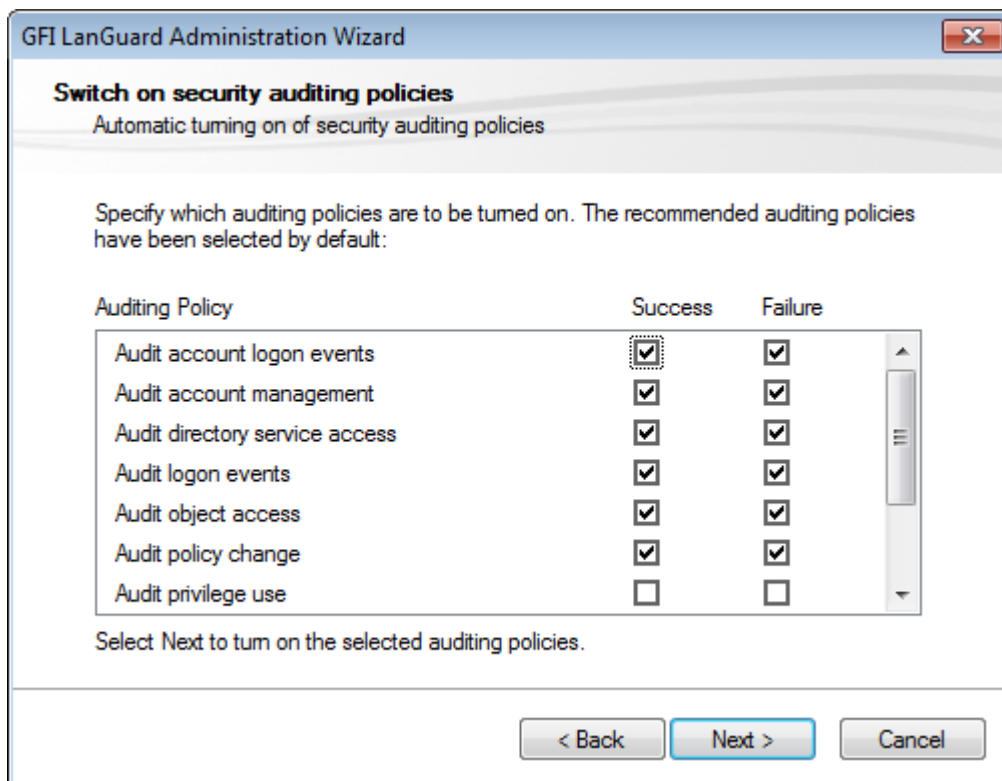
Security audit policy

An important part of any security plan is the ability to monitor and audit events on your network. These event logs are frequently referenced to identify security holes or breaches. Identifying attempts and preventing them from becoming successful breaches of your system security is critical. In Windows, you can use 'Group Policies' to set up an audit policy that can track user activities or system events in specific logs.

To keep track of your system auditing policy, GFI LanGuard collects the security audit policy settings from target computers and includes them in the scan result. To access more information on the result click on  Security Audit Policy sub-node.

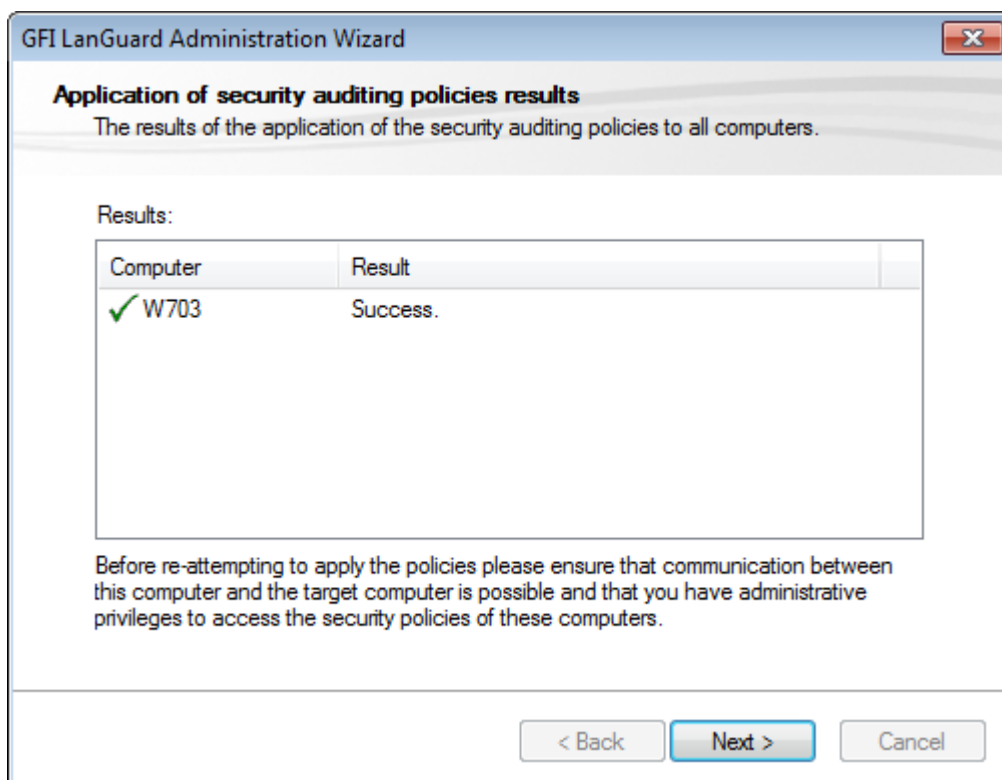
Apart from gaining knowledge on the current audit policy settings, you can also use GFI LanGuard to access and modify the audit policy settings of your target computers. To achieve this:

1. From the **Scan Results Overview** panel, right-click on the respective target computer and select **Enable auditing on ► This computer/Selected computers/All computers**.



Screenshot 28 - The audit policy administration wizard

2. Select/unselect auditing policies accordingly, and click **Next** to deploy the audit policy configuration settings, on the target computer(s).



Screenshot 29 - Results dialog in audit policy wizard

3. At this stage, a dialog will show whether the deployment of audit policy settings was successful or not. To proceed to the next stage click **Next**. Click **Back** to re-deploy settings on failed computers.

4. Click **Finish** to finalize configuration.

Groups/users

Rogue, outdated or default user accounts can be exploited by malicious or unauthorized users to gain access to restricted areas of your IT infrastructure. The 'Guest' account for example is just one commonly exploited accounts; more often than not, this account is left configured within a system and even worse without changing the default password settings. Malicious users have developed applications that can automatically re-enable the 'Guest' account and grant it administrative rights. This empowers users to gain access to sensitive areas of the corporate IT infrastructure.

GFI LanGuard collects information on all user accounts and user groups currently enabled on scanned targets. This information is organized in the scan results under two separated nodes. To access the list of user accounts identified during on a target computer, click  **Users** sub-node. Use the information enumerated in this sub-node to inspect the access privileges assigned to each user account. To gain access to the list of user-groups configured on a target computer, click  **Groups** sub-node.



Users should not use local accounts to log on to a network computer. For better security, users should log on to network computers using a 'Domain' or an 'Active Directory' account.

Sessions

Click  **Sessions** sub-node to access the list of hosts that were remotely connected to the target computer during scanning.



The information included in this sub-node also includes the remote connection details of the scanning sessions just performed by GFI LanGuard. For example, the IP of the computer running LanGuard, logon credentials and other related information.

Services

Active services can be a potential security weak spot in your network system. Any of these services can be a Trojan, a virus or another type of malware, that can seriously affect your system in a dangerous way. Furthermore, unnecessary applications and services that are left running on a system consume valuable system resources.

During the scanning process, GFI LanGuard enumerates all services running on a target computer for you to analyze. This way you can identify the services to stop. Further to the freeing up of resources, this exercise automatically hardens your network by reducing the entry points through which an attacker can penetrate into your system. To access the list of services enumerated during a scan, click  **Services** sub-node.

Processes

Click  **Processes** sub-node to access the list of processes running on the target computer during a scan.

Remote time of day

Click  **Remote TOD (time of the day)** sub-node to view the network time that was read from the target computer during the scan. This time is generally set on network computers by the respective domain controller.

4 Analyzing Results

4.1 Introduction

The **Dashboard** section provides you with extensive security information based on data acquired during audits. Amongst others, the **Dashboard** section enables you to determine the current network vulnerability level, the top-most vulnerable computers, and the number of computers in the database. To display the **Dashboard** section:

1. Launch GFI LanGuard management console and from the **Home** page select **View Dashboard**.



Screenshot 30 - View Dashboard

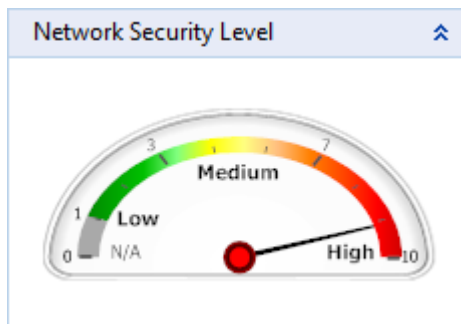
2. From the **Dashboard** tab, select one of the options described in the following sections:

4.1.1 Overview

The **Dashboard Overview** is a graphical representation of the security level/vulnerability level of a single computer, domain or entire network.

When a computer or domain is selected, the results related to the selected computer/domain are automatically updated in the dashboard. Below is a description of each section found in the dashboard:

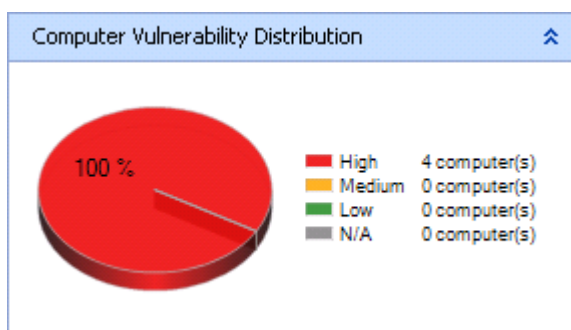
Network security level



Screenshot 31 - Network Security Level

This rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found. A high vulnerability level is a result of vulnerabilities and/or missing patches which average severity is categorized as high.

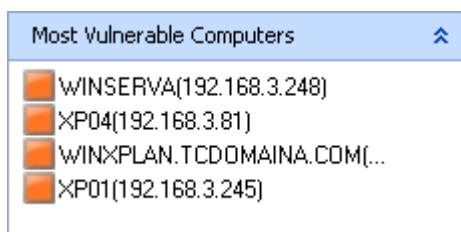
Computer vulnerability distribution



Screenshot 32 - Computer Vulnerability Distribution

This chart is available only when selecting a domain or a workgroup, and displays the distribution of vulnerabilities on your network. This chart enables you to determine how many computers have high, medium and low vulnerability rating.

Most vulnerable computers

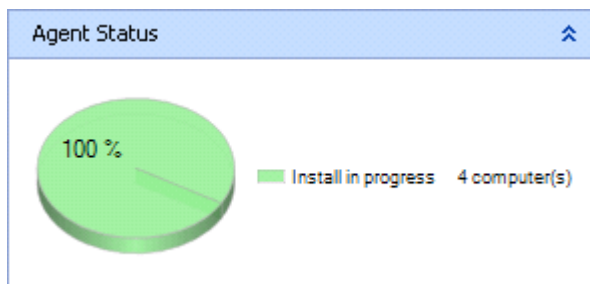


Screenshot 33 - Most Vulnerable Computers

This list is available only when selecting a domain or a workgroup, and shows the most vulnerable computers discovered during the scan. The icon color on the left indicates the vulnerability level.

Agent status

When selecting a domain or workgroup, a chart showing the overall agent status of all computers within the domain/workgroup is displayed. This enables you to determine the number of agents installed or pending installation on the selected domain/workgroup.



Screenshot 34 - Agent Status when selecting a domain/workgroup

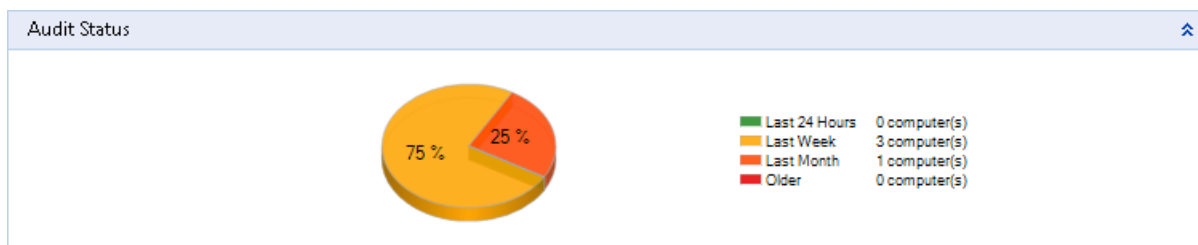
When selecting a single computer, this section displays an icon representing the agent status. The icons are described in Table 19 below:

Table 19 - Agent status

ICON	STATUS NAME	DESCRIPTION
	Not installed	Agent is not installed on the target machine.
	Pending installation	Installation is pending. A status can be pending when the machine is offline or the agent is being installed.
	Pending uninstall	Uninstallation is pending. A status can be pending when the machine is offline or the agent is being uninstalled.
	Installed	Agent is installed on the target machine.

Audit status

This chart is available only when selecting a domain or workgroup and enables you to identify how many audits have been performed on your network grouped by time.



Screenshot 35 - Audit status chart

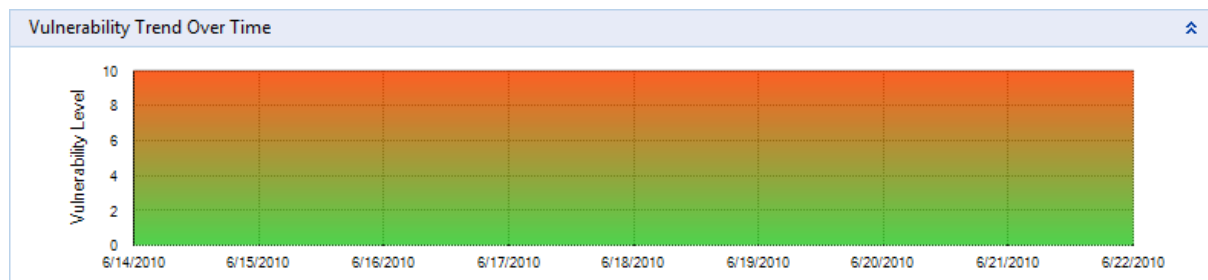
Vulnerability trends over time

When a domain or workgroup is selected, this section displays a line graph showing the change of vulnerability level over time grouped by computer count.



Screenshot 36 - Vulnerability Trends Over Time for a domain/workgroup

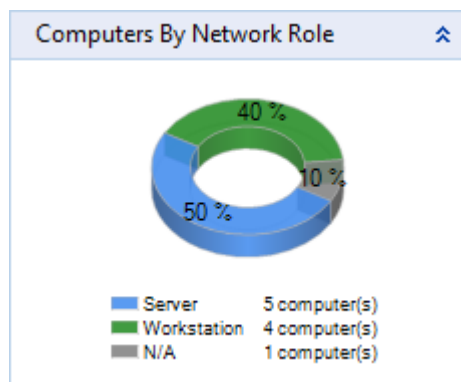
When a single computer is selected, this section displays a graph showing the change of vulnerability level over time for the selected computer.



Screenshot 37 - Vulnerability Trends Over Time for a single computer

Computers by network role

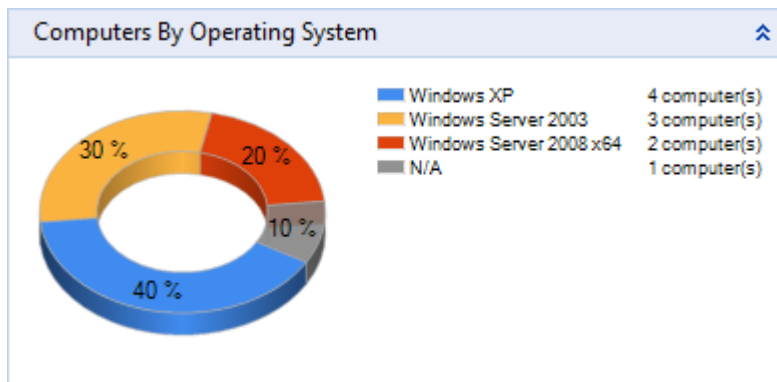
This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by network role. Amongst other roles, this graph identifies the number of servers and workstations per selected domain.



Screenshot 38 - Computers by network role

Computers by operating system

This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by the installed operating system.



Screenshot 39 - Computers by operating system

Computer details

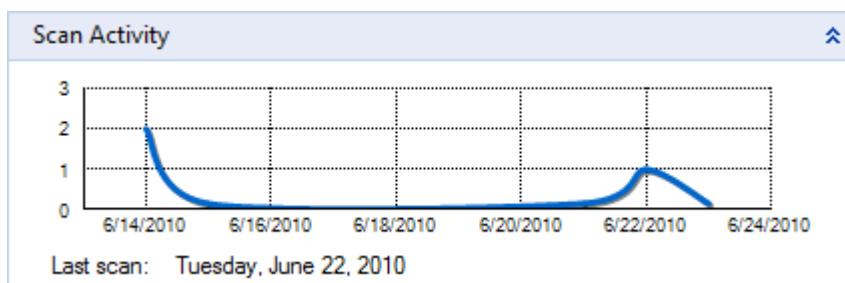
This section is available when selecting a single computer and enables you to view the selected computer details.

Computer Details	
Computer name	WINSERVA
IP address	192.168.3.248
MAC	01-02-5F-5F-4D-53
Operating system:	Windows Server 2003
Network role	PDC (Primary Domain Controller)
Virtual machine	Microsoft Virtual PC
Language	EN

Screenshot 40 - Computer Details

Scan activity

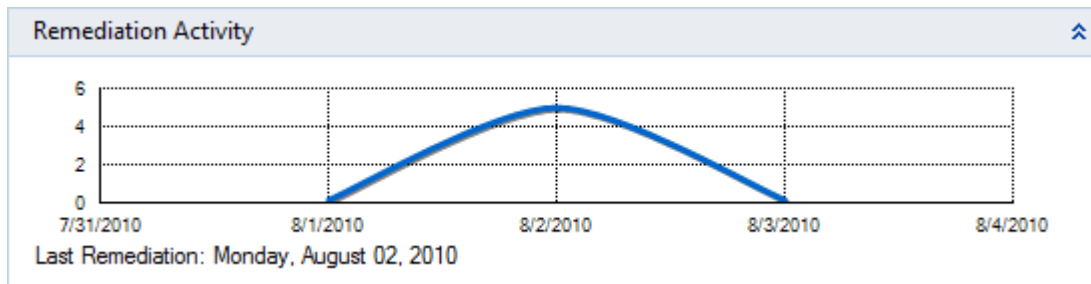
This line graph is available only when selecting a single computer and enables you to view the number of scans/audits performed on the selected computer. In addition enables you to verify if scheduled scans are being performed.



Screenshot 41 - Scan activity

Remediation Activity

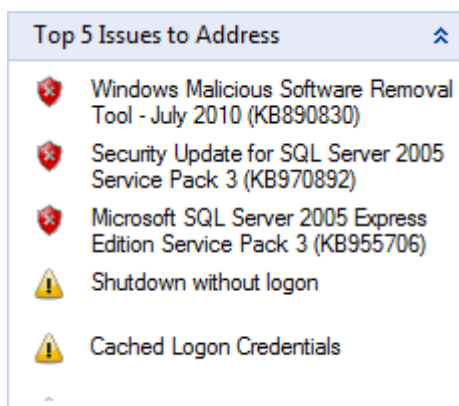
This line graph is available only when selecting a single computer and enables you to view the number of remediation activities performed on the selected computer. In addition, this graph enables you to verify that auto-remediation is performed.



Screenshot 42 - Remediation activity

Top 5 Issues to Address

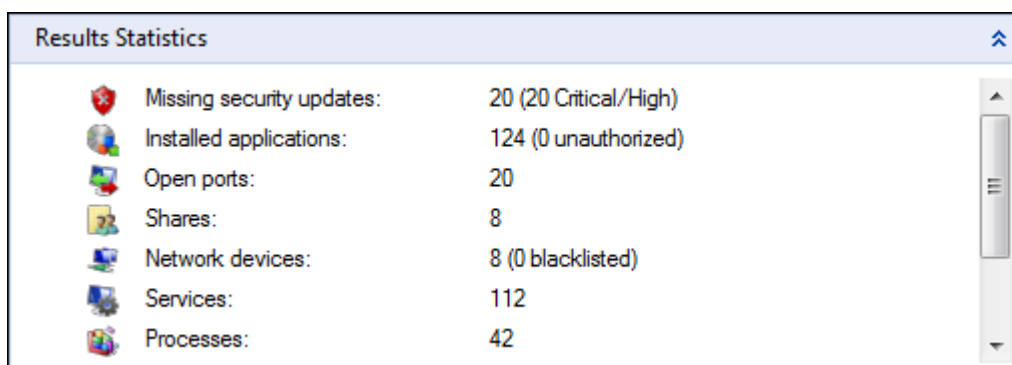
This section is available only when selecting a single computer, and displays the top five issues to address for the selected computer.



Screenshot 43 - Top 5 issues to address

Results statistics

This section is available only when selecting a single computer and displays an overview of the audit result. Amongst others, the result enables you to identify the number of missing patches, number of installed applications, open ports and running services.



Screenshot 44 - Result statistics

4.2 Computers view

WORKGROUP - 28 computers Search Entire Network

Overview **Computers** History Vulnerabilities Patches Ports Software Hardware System Information

Additional Information Categories: Agent Details

Drag a column header here to group by that column

Computer...		General Information							
VL	Co... Name	Domain	...	OS	SP	Last Discovery	Last Audit	Credentials	Agent
	W703	WORKGROUP	-	Windows 7	Gold	04/08/2011 18:35	04/08/2011 18:35	✓ Not Set	Not Installed
	TEMP	WORKGROUP	-	Windows 7	Gold	09/08/2011 00:43	09/08/2011 00:37	✓ Not Set	Not Installed
	RES...	WORKGROUP	-	N/A	-	04/08/2011 21:59	04/08/2011 21:59	✗ Not Set (errors enc...	Not Installed
	W701	WORKGROUP	-	N/A	-	04/08/2011 22:52	04/08/2011 22:52	✗ Not Set (errors enc...	Not Installed
	GFI...	WORKGROUP	-	N/A	-	04/08/2011 21:22	04/08/2011 21:22	✗ Not Set (errors enc...	Not Installed
	BAJ...	WORKGROUP	-	N/A	-	04/08/2011 21:22	04/08/2011 21:22	✗ Not Set (errors enc...	Not Installed
	GFI...	WORKGROUP	-	N/A	-	04/08/2011 21:22	04/08/2011 21:22	✗ Not Set (errors enc...	Not Installed
	GFI...	WORKGROUP	-	N/A	-	04/08/2011 21:28	04/08/2011 21:28	✗ Not Set (errors enc...	Not Installed
	ARI...	WORKGROUP	-	N/A	-	04/08/2011 21:30	04/08/2011 21:30	✗ Not Set (errors enc...	Not Installed
	GX620	WORKGROUP	-	N/A	-	04/08/2011 21:34	04/08/2011 21:34	✗ Not Set (errors enc...	Not Installed
	OW...	WORKGROUP	-	N/A	-	04/08/2011 21:37	04/08/2011 21:37	✗ Not Set (errors enc...	Not Installed
	RES...	-	-	N/A	-	-	-	✗ Not Set (errors enc...	Not Installed
	PSGC1	WORKGROUP	-	N/A	-	04/08/2011 21:43	04/08/2011 21:43	✗ Not Set (errors enc...	Not Installed
	RES...	WORKGROUP	-	N/A	-	04/08/2011 21:54	04/08/2011 21:54	✗ Not Set (errors enc...	Not Installed
	PSG...	-	-	N/A	-	-	-	✓ Not Set	Not Installed
	RES...	WORKGROUP	-	N/A	-	04/08/2011 22:01	04/08/2011 22:01	✗ Not Set (errors enc...	Not Installed

Co...

Screenshot 45 - Analyze results by computer

Select this view to group audit results by computer. From the drop down list, select one of the options described in Table 20 below to view related information:

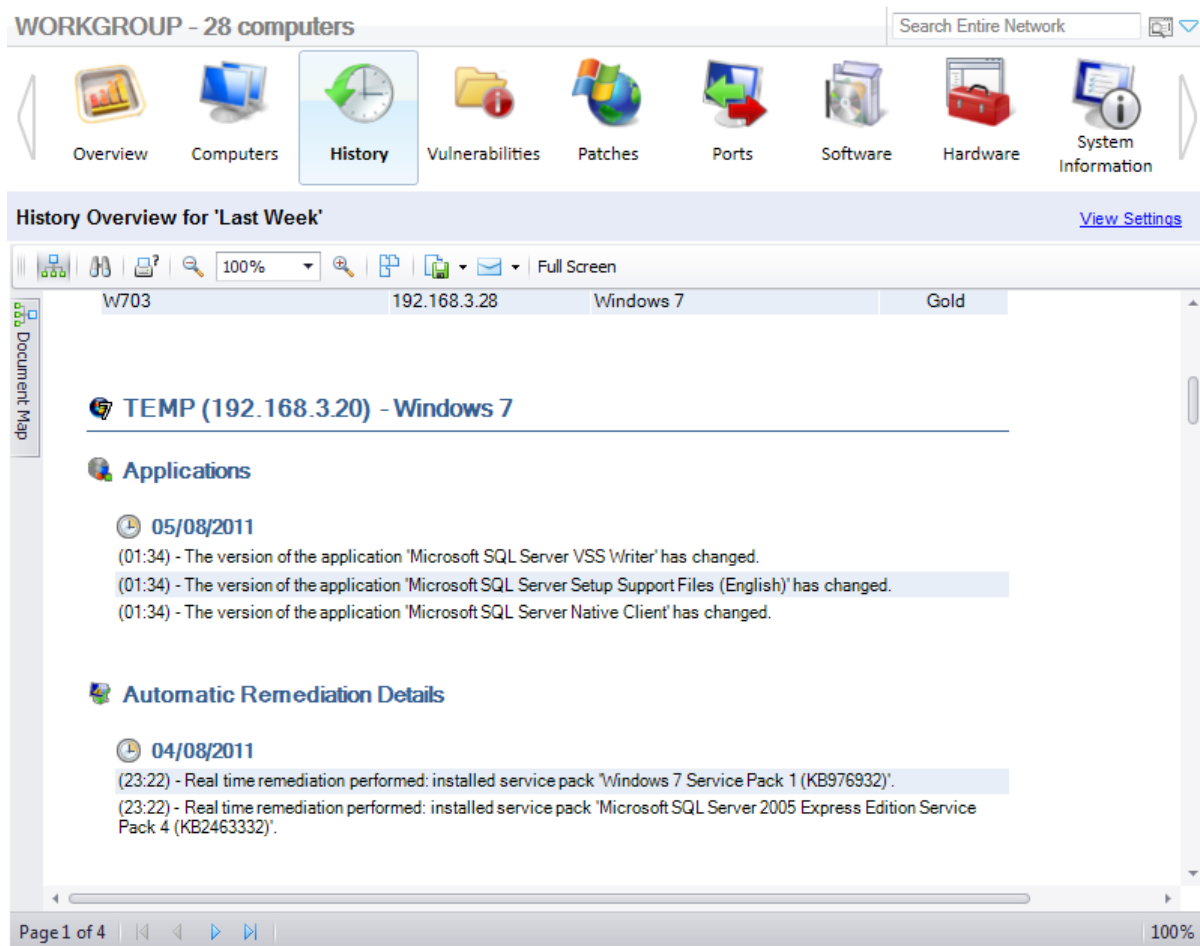
Table 20 - View by computers information

OPTION	DESCRIPTION
General information	Select this option to display information on the: » Domain name » Operating system » Service pack installed » Last scan date and time » Operating system language NOTE: Server and VM columns enable you to identify if the selected computer is a server or a virtual machine respectively.
Agent Details	Select this option to view the agent status. This option enables you to identify if an agent is installed on a computer and if yes, displays the type of credentials being used by the agent.

OPTION	DESCRIPTION
Vulnerabilities	View the number of vulnerabilities found on a computer grouped by severity. Severity of a vulnerability can be: » High » Medium » Low » Potential For a full description of each rating, refer to Vulnerability assessment section in this manual.
Patching status	View the number of: » Missing patches » Missing service packs » Installed patches » Installed service packs
Open ports	View the number of: » Open TCP ports » Open UDP ports » Backdoors
Software	View the number of: » Antiphishing engines » Antispyware engines » Antivirus engines » Backup applications » Data loss prevention applications » Device access and disk encryption applications » Firewalls » Installed applications » Instant messengers » Peer to peer applications » Unauthorized applications » Virtual machines » VPN clients » Web browsers
Hardware	View information on: » Number of disk drives » Free disk space » Memory size » Number of processors » Other hardware.
System information	View information on: » The number of shared folders » Number of groups » Number of users » Logged users » Audit policy status.

4.3 History view

Select this view to group audit results by date for a specific computer. To configure the history starting date or history period click the link provided.



Screenshot 46 - Dashboard: History

4.4 Vulnerabilities view

Display more details on the vulnerabilities found on a network and the number of affected computers. When a vulnerability is selected from the **Vulnerability List**, the **Details** section provides more information on the selected vulnerability. From the **Details**, section click **View affected computers** or **View unaffected computers** to display a list of affected and unaffected computers. For a description of terms used in this result, refer to [Vulnerability assessment](#).

WORKGROUP - 28 computers Search Entire Network

Overview Computers History **Vulnerability...** Patches Ports Software Hardware System Information

Vulnerability Types

- High Security Vulnerabilities (9)
- Medium Security Vulnerabilities (18)
- Low Security Vulnerabilities (11)
- Potential Vulnerabilities (4)
- Missing Patches (50)
- Missing Service Packs (2)
- Firewall Vulnerabilities (1)

Vulnerability List

Drag a column header here to group by that column

Vulnerability name	Product	No. of computers
All Servers: Adcycle - build.cgi	Adcycle	1
All Servers: Brian Stanback bsgue...		1
All Servers: Brian Stanback bslist.cgi		1
All Servers: DCShop vulnerability	DCShop	1
All Servers: Free On-line Dictionary		1
Leif M. Wright ad.cgi		1
OWASP: 12219: Untrusted search p...	Microsoft Office PowerPoint 2007	1

Count=9

Details

 **High Security Vulnerability:** All Servers: Adcycle - build.cgi

Type: Web
Date: 20 November 2000
Product: Adcycle
Description: Build.cgi if it has execute permission and is in the cgi directory, passwords can be compromised and remote users can delete your data.
References: [CVE-2000-1161](#), [SecurityFocus-1969](#)

[View affected computers](#)
[View unaffected computers](#)

Screenshot 47 - Dashboard: Vulnerabilities

4.5 Patches view

Display more details on the missing/installed patches and service packs found during a network audit. When a patch/service pack is selected from the **List**, the **Details** section provides more information on the selected patch/service pack. From the **Details** section, click **View computers having this patch missing** to display a list of computers having the selected patch missing. For a description of terms used in this result, refer to [System Patching Status](#) section in this manual.

WORKGROUP - 28 computers Search Entire Network

Overview Computers History Vulnerabilities **Patches** Ports Software Hardware System Information

Patch Types

- Missing Patches (50)
- Missing Service Packs (2)
- Installed Patches (50)
- Installed Service Packs (3)

Patch List

Drag a column header here to group by that column

Patch name	Date posted	Severity	Applies to	No. of computers
APSB11-18: Adob...	2011-06-28	Critical	Adobe Flash Playe...	1
MS07-025: Securi...	2007-05-15	Important	Office	1
MS07-036: Securi...	2007-07-10	Important	Office	1
MS07-036: Securi...	2007-07-10	Important	Office	1
MS07-037: Securi...	2007-07-10	Important	Office	1
MS07-042: Securi...	2007-08-14	Important	Office	1
MS08-015: Securi...	2008-03-11	Critical	Office	1

Count=50

Details

Missing Patch: APSB11-18: Adobe Flash Player 10.3.181.34 [Remediate](#)

Bulletin ID: APSB11-18
QNumber: APSB11-18
Date: 28 June 2011
Severity: Critical
Applies to: Adobe Flash Player 10
Description: This release contains fixes for critical vulnerabilities identified in Security Bulletin APSB11-18. All users are encouraged to update to the new players version 10.3.181.34.
URL: <http://www.adobe.com/support/security/bulletins/apsb11-18.html>
Note: Before distributing this software in you network make sure you agree and comply with Adobe license. More details here: <http://www.adobe.com/licensing/>

Screenshot 48 - Dashboard: Patches

4.6 Ports view

Display more details on the open ports found during a network audit. When a port is selected from the **Port List**, the **Details** section provides more information on the selected port. From the **Details** section, click **View computers having this port open** to display a list of computers having the selected port open. For a description of terms used in this result, refer to [Ports](#) section in this manual.

WORKGROUP - 28 computers Search Entire Network

Overview Computers History Vulnerabilities Patches **Ports** Software Hardware System Information

Port Types

- Open TCP Ports (67)
- Open UDP Ports (43290)

Port List

Drag a column header here to group by that column

Port	Process	No. of computers
TCP 21		2
TCP 25		3
TCP 80		11
TCP 135		17
TCP 135	svchost.exe	1
TCP 139		20
TCP 443		3
TCP 445		19
TCP 445	System	1

Count=67

Details

Open TCP Port: TCP 21

Type: TCP

Port number: 21

[View computers having this port open](#)

Screenshot 49 - Dashboard: Ports

4.7 Software view

Display more details on the installed applications found during a network audit. When an application is selected from the **Application List**, the **Details** section provides more information on the selected application. For a description of terms used in this result, refer to [Software](#) section in this manual.

WORKGROUP - 28 computers Search Entire Network

Overview Computers History Vulnerabilities Patches Ports **Software** Hardware System Information

Application Category

- All Applications (25)
- Antispyware (1)
- Antiphishing (1)
- Firewall (1)
- VPN Client (1)
- Web Browser (1)
- Disk Encryption (1)
- Patch Management (3)

Applications List

Drag a column header here to group by that column

Application name	Version	Publisher	No. of computers
Adobe Flash Player 10 ActiveX	10.1.82.76	Adobe Systems ...	1
Alchemy Catalyst 9.0	9.00.0000	Alchemy Softwa...	1
Alchemy Publisher 3.0	3.00.0000	Alchemy Softwa...	1
Camtasia Studio 7	7.1.0	TechSmith Corp...	1
FastStone Capture 6.7	6.7	FastStone Soft	1
GFI LanGuard 2011	10.1.2011.0802	GFI Software Ltd	1
HTML Help Workshop			1
MadCap Lingo V4	4.0.0	MadCap Software	1
Microsoft .NET Framework 4 ...	4.0.30319	Microsoft Corpo...	2

Count=25

Details

 **Application:** Adobe Flash Player 10 ActiveX

Version: 10.1.82.76

Publisher: Adobe Systems Incorporated

[View computers with Adobe Flash Player 10 ActiveX installed](#)

[View computers without Adobe Flash Player 10 ActiveX installed](#)

Screenshot 50 - Dashboard: Software

4.8 Hardware view

Display more information on the hardware found during a network audit. Select hardware from the List to display more details. For a description of terms used in this result, refer to [Hardware](#) section in this manual.

WORKGROUP - 28 computers Search Entire Network

Overview Computers History Vulnerabilities Patches Ports Software **Hardware** System Information

Hardware Types

- Network Devices (24)
- Processors (1)
- Motherboards (1)
- Storage Devices (5)
- Display Adapters (1)
- Local Drives (4)
- Other Devices (45)
- Memory (1)

Hardware List

Drag a column header here to group by that column

	Hardware name	Type	Vendor	No. of computers
	Microsoft ISATAP Adapter	Virtual devices	Microsoft	1
	Microsoft ISATAP Adapter	Unknown	Microsoft	1
	Microsoft ISATAP Adapter #2	Virtual devices	Microsoft	1
	Microsoft Virtual Machine Bus Net...	Physical de...	Microsoft	1
	Microsoft Virtual Machine Bus Net...	Physical de...	Microsoft	1
	Microsoft Virtual Machine Bus Net...	Unknown	Microsoft	1
	RAS Async Adapter	Software e...	Microsoft	1
	Teredo Tunneling Pseudo-Interface	Unknown	Microsoft	1
	WAN Miniport (IKEv2)	Virtual devices	Microsoft	1
	WAN Miniport (IKEv2)	Unknown	Microsoft	1

Count=24

Details

Network Device: Microsoft ISATAP Adapter

Typ: Virtual devices
Hersteller: Microsoft

[View affected computers](#)
[View unaffected computers](#)

Screenshot 51 - Dashboard: Hardware

4.9 System Information

The **System Information** tab, displays information associated with the operating system of a scan target(s). For a description of terms used in this result, refer to [System Information](#) section in this manual.

System Information Types

- Shares (8)
- Services (171)
- Processes (45)
- Users (5)
- Logged On Users (6)
- User Groups (19)

System Information List

System information name	No. of computers
ADMIN\$	4
C\$	4
G\$	1
IPC\$	5
Music	1
print\$	1
Print_to_PDF	1
Users	3

Count=8

Details

Shares ADMIN\$

[Show computers that have this item](#)

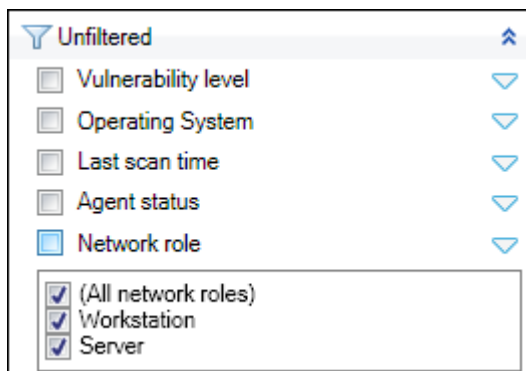
[Show computers that do not have this item](#)

Screenshot 52 - Dashboard: System information

4.10 Display results

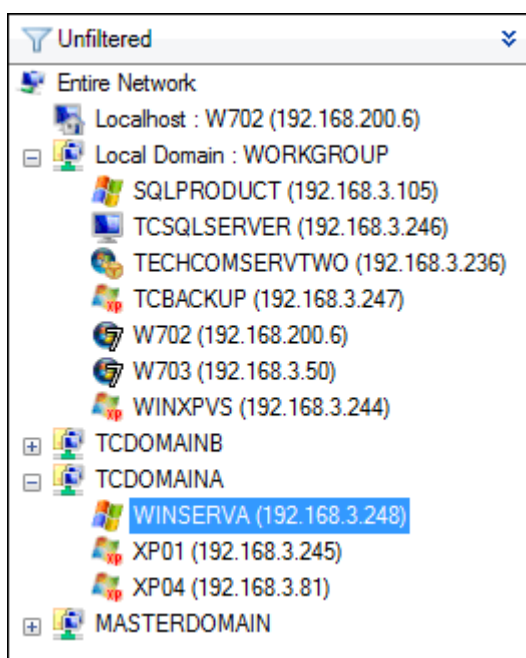
GFI LanGuard includes a filtering option that allows you to quickly find a computer or domain and immediately display the results. To display the result for a particular domain or computer:

1. Click **Dashboard** tab.
2. From the left panel select the filtering criteria. Select between the pre-defined criteria or click **Advanced filtering** to add additional criteria.



Screenshot 53 - Dashboard filtering criteria

3. From the left panel select the computer\domain. The dashboard automatically updates the results on selection.



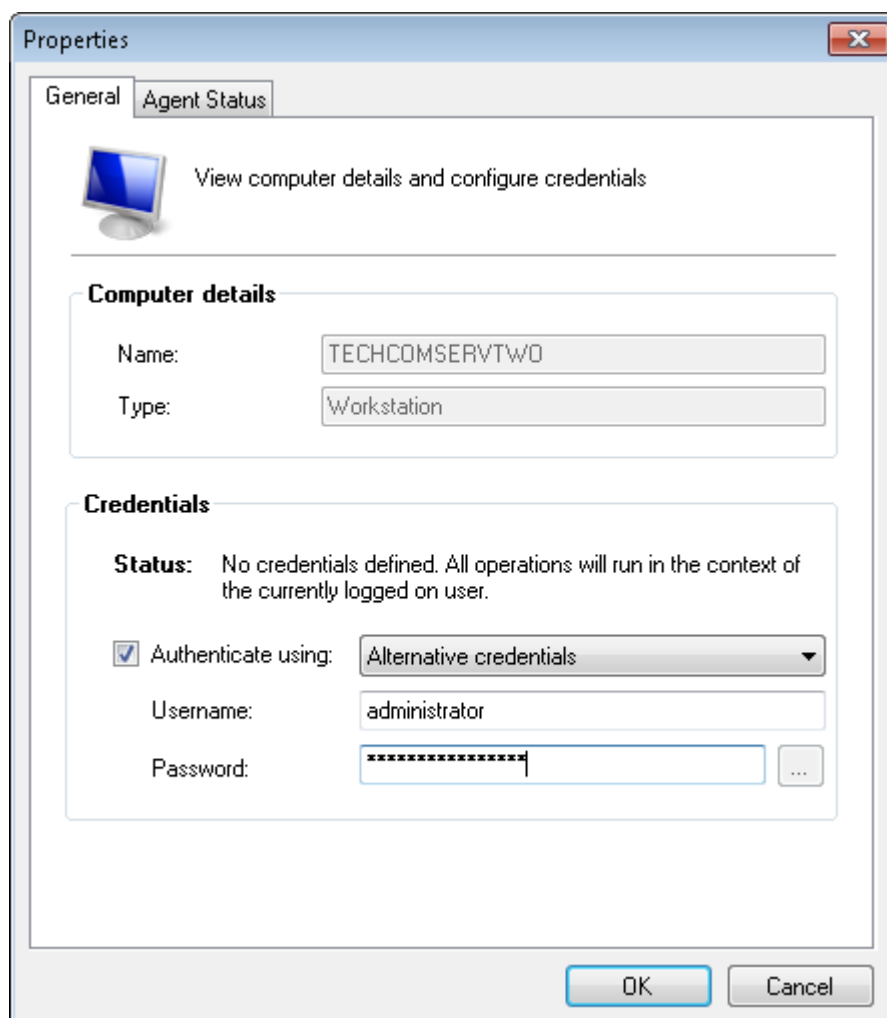
Screenshot 54 - Computer\Domain list

4.11 Configure credentials

Regardless of the network size, systems administrators typically have to use different sets of credentials for different computers. Systems (such as Linux-based environments) often use of special authentication methods such as public key authentication. Such methods generally also require special/custom logon credentials, (for example, private key files) instead of the conventional password strings.

The GFI LanGuard Dashboard enables you can configure a different set of logon credentials for each computer to scan. The scanning engine will use the specified credentials to authenticate on target computers.

1. From GFI LanGuard home page, select **View Dashboard**.
2. From the left panel, right-click a computer or domain and select **Properties**.



Screenshot 55 - Configuring computer credentials

3. From the **Credentials** section, select **Authenticate using** checkbox to configure the authentication method. Table 21 below describes the available authentication methods:

Table 21 - Authentication methods

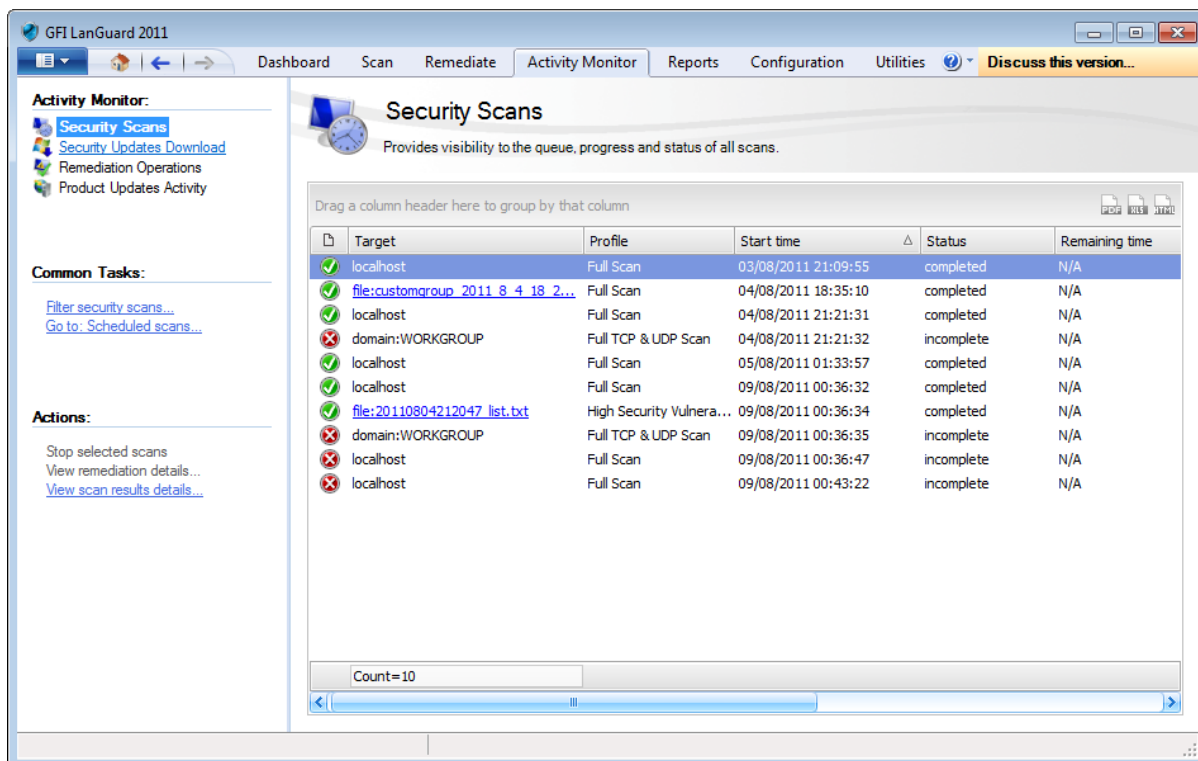
OPTION	DESCRIPTION
Currently logged on user	Uses the currently logged on user credentials when logging on target machines.
Alternative credentials	Uses custom credentials. Key-in the user name and password to use.
A null session	Logs in target machines using a null session. User will log into the target machine as an anonymous user.
A private key file	Uses SSH private key authentication (Linux-based systems). A username and a key file are required.

4. Click **OK**.

4.12 Monitoring activity

Scheduled Activity is all the GFI LanGuard operations that have been set up to trigger at a later date and time. To view current activity:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Activity Monitor** tab.



Screenshot 56 - Action Center: Scheduled Activity

3. From the left pane, select one of the following views:

- » Security Scans
- » Security Updates Downloads
- » Remediation Operations
- » Product Updates Activity

This section describes each option in more details.

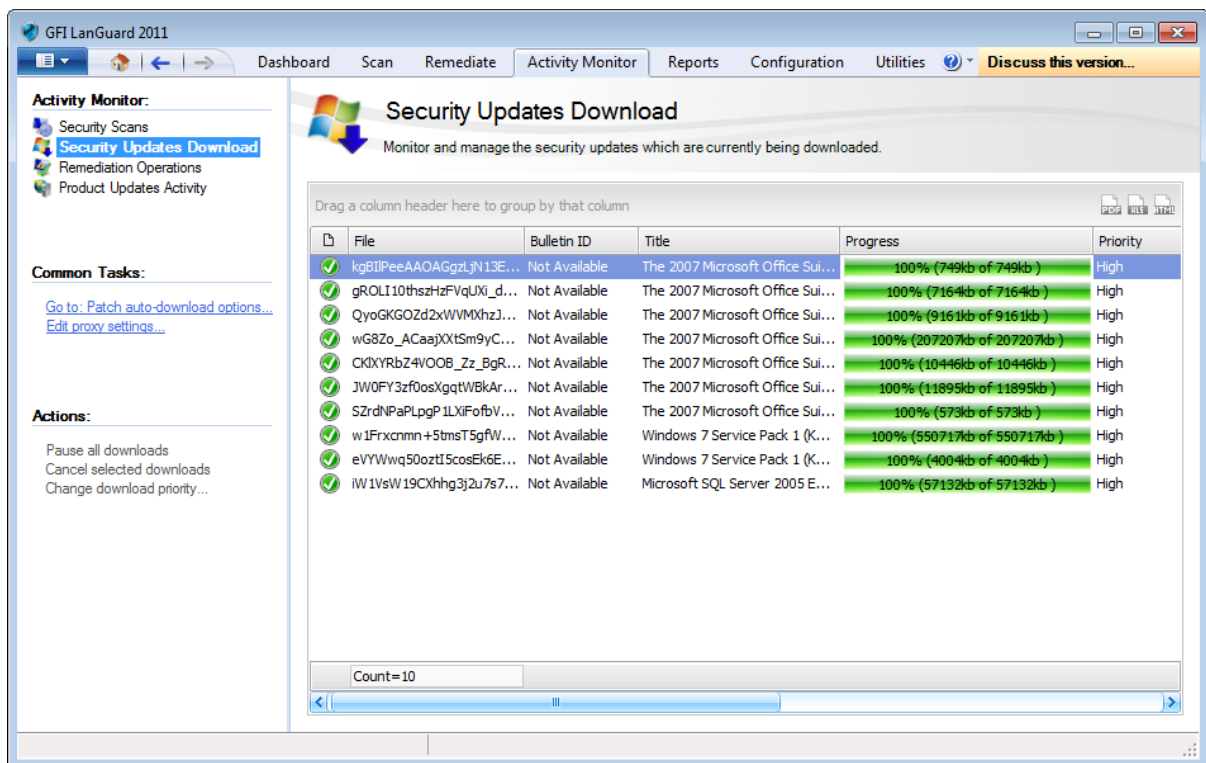
Security Scans

The **Security Scans** section enables monitoring of all the security scans that are currently in progress. To stop a scan right-click the security scan and select **Stop selected scans** option.

For more information on how to set up a new scheduled scan, refer to [Setting up a scheduled scan](#) section in this manual.

Security Updates Downloads

The Security Updates Downloads screen enables you to monitor, pause, cancel or change priority to all the scheduled patch downloads.



Screenshot 57 - Security updates download

The icon in the first column indicates the download status. Table 22 below describes the different status:

Table 22 - Updates download status

ICON	DESCRIPTION
	Downloaded - Update downloaded successfully.
	Downloading - Update is being downloaded.
	Failed - An error occurred while downloading the update.
	Pending - Update is queued for download.
	Cancelled - User canceled update download.

Right-click an entry and select one of the options described in Table 23 below:

Table 23 - Security updates download

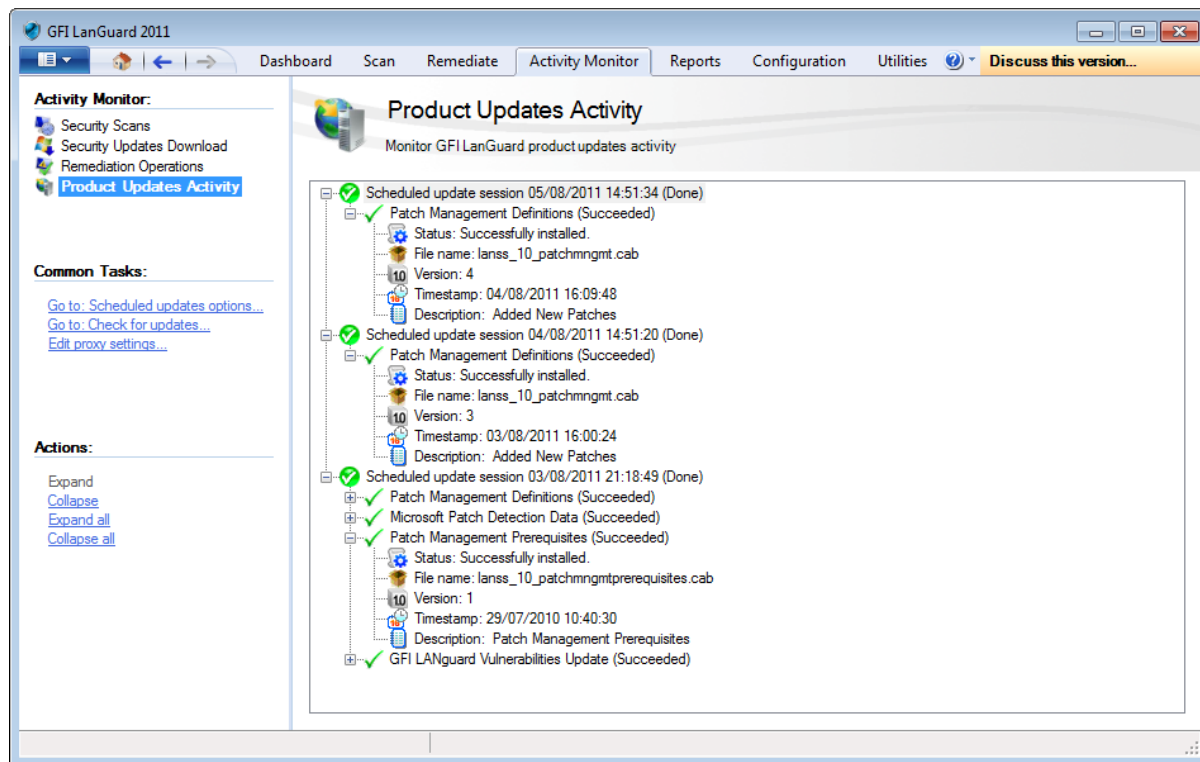
OPTION	DESCRIPTION
Configure Patch Auto-Download	Enables or disables auto-patch download and used to configure where the patches are stored. For more information, refer to Patch Auto-download settings section in this manual.
Edit proxy settings...	Configure the proxy settings used by GFI LanGuard to connect to the Internet. For more information, refer to Configure GFI LanGuard Proxy settings section in this manual.
Change download priority...	Change the download priority. Select between, High, normal or low priority.
Cancel selected downloads	Stop and remove the selected download.
Pause all downloads	Temporarily pause all downloads.

Remediation Operations

The remediation operations screen enables you to monitor as well as cancel all the scheduled remediation features within GFI LanGuard. For more information on how to fix vulnerabilities, refer to [Fixing vulnerabilities](#) section in this manual.

Product Updates Activity

The Product updates activity screen enables you to monitor or edit GFI LanGuard scheduled or manual updates. For more information on how to set up scheduled or manual updates, refer to [Program updates](#) section in this manual.



Screenshot 58 - Product updates activity

5 Fixing Vulnerabilities

5.1 Introduction

GFI LanGuard enables you to automatically fix some of the issues identified during your network audit using the built-in tools that ship with the product. Available actions include:

Table 24 - Automatic remediation actions

OPTION	DESCRIPTION
Auto-patch management	Downloads missing updates and deploys them over the network.
Applications auto-uninstall	Auto-uninstall of applications that support silent uninstall. The process involves a test phase (called validation) during which an application is uninstalled automatically to identify if silent uninstall is supported by target application. If it is, all the other instances on the network are automatically uninstalled during a scan.

5.2 Automatic-Remediation

Automatic-Remediation enables you to automatically download and deploy missing patches as well as uninstall unauthorized applications during scheduled operations.

To uninstall software, a 3-stage process is required in order to identify whether the selected application supports silent uninstall:

Table 25 - Automatic remediation stages

STAGE	DESCRIPTION
Stage 1	Select the application to auto-uninstall.
Stage 2	Ensure that application supports silent uninstall. Test this by trying to remotely uninstall the application. This is the validation process.
Stage 3	Setup a scheduled audit that will remove the unauthorized application. This is done automatically (using agents) or manually (agent-less approach).

	Auto-remediation and un-installation of un-authorized applications only work with scanning profiles that detect missing patches and/or Installed applications.
	Always test patches in a test environment before deployment.
	By default, Microsoft updates are not enabled for automatic deployment. Manually approve each patch (as it is tested) or set all Microsoft updates as approved.

5.2.1 Automatically deploy missing updates

To deploy missing patches automatically, follow the instructions below before configuring a scan with auto-remediation options.

Approve the patches to deploy automatically

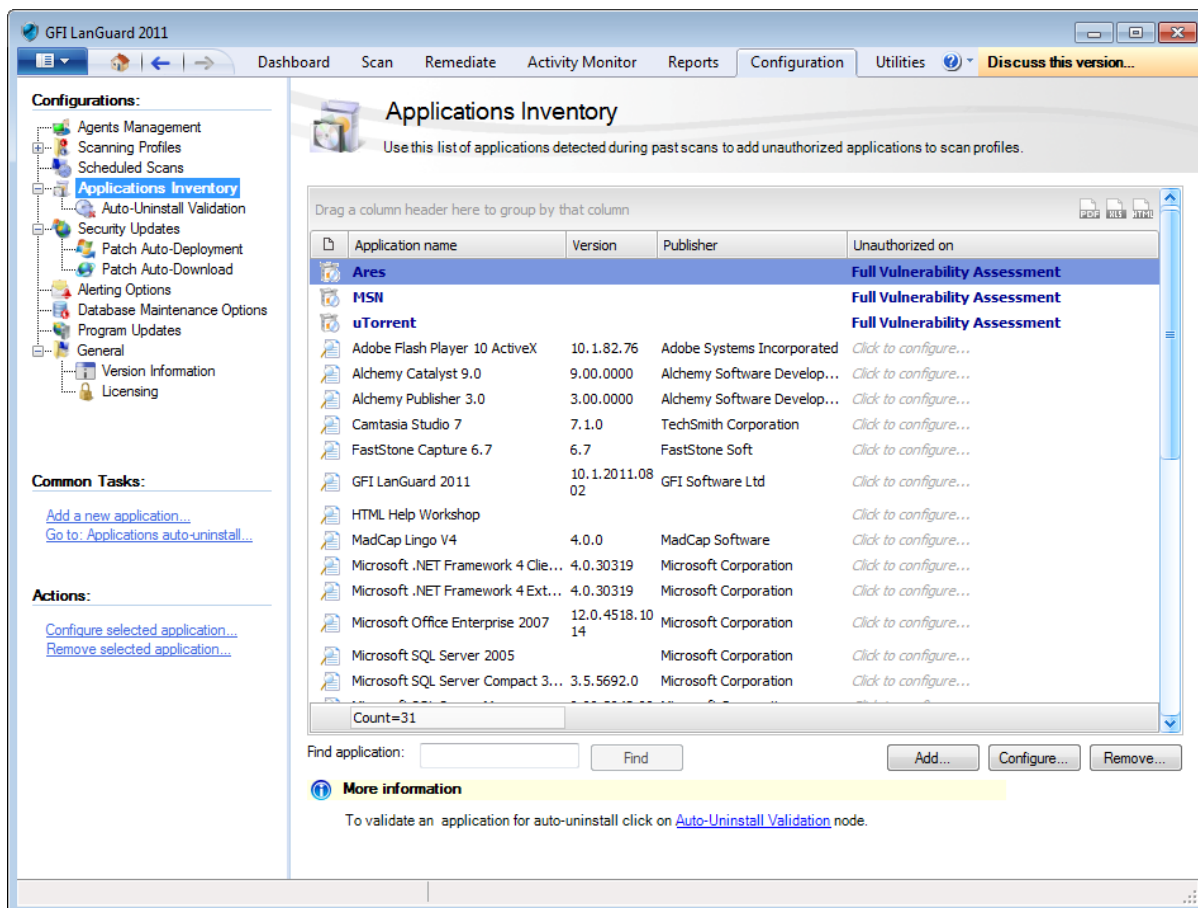
1. From the **Configuration** tab, navigate to **Security Updates ► Patch Auto-Deployment**.
2. Select the patches to approve for auto-deployment. Optionally, set the automatic patch approval options by selecting **To automatically approve patches and/or service packs, click here** option. For more information, refer to the [Auto-deployment settings](#) section in this manual.

5.2.2 Automatically uninstall unauthorized applications

To uninstall unauthorized applications automatically follow the instructions below before setting up a scan with auto-remediation options.

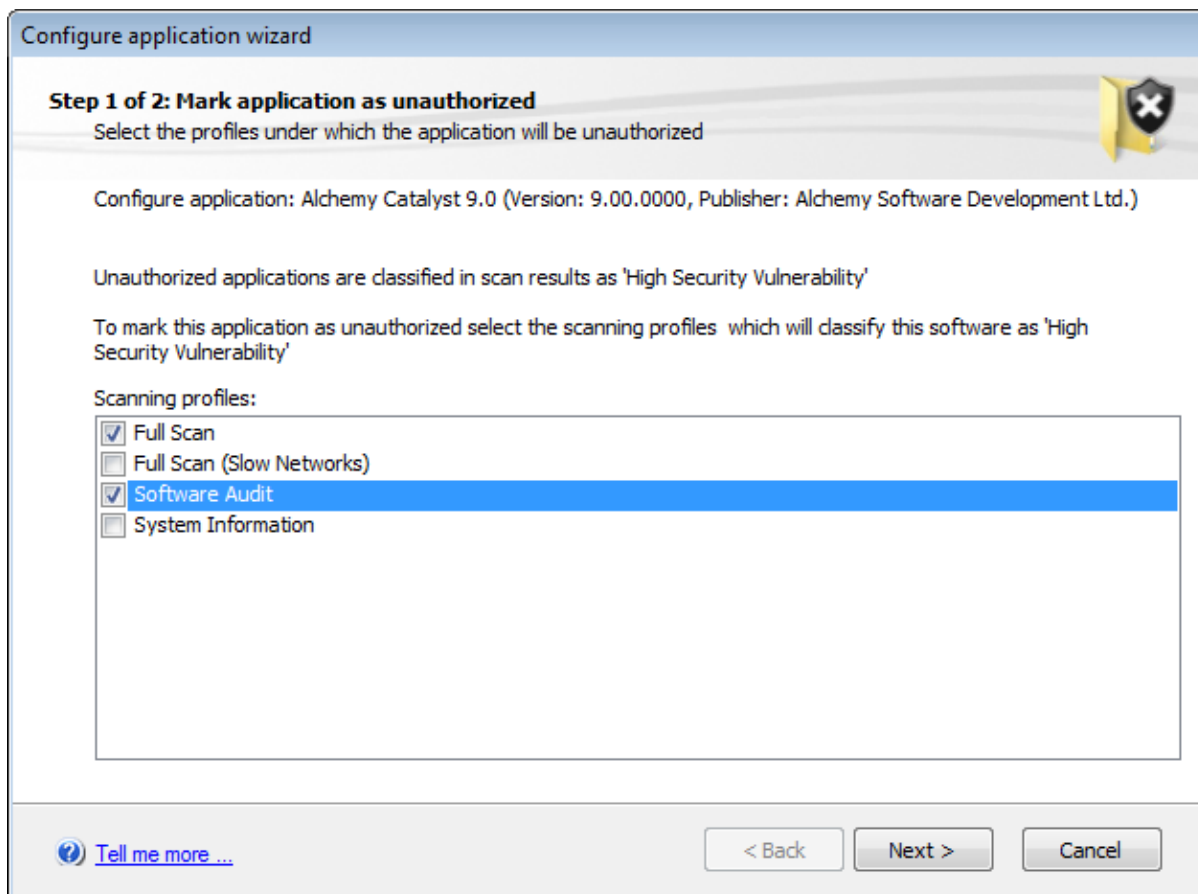
To define unauthorized applications list:

1. From the **Configuration** tab, select **Applications inventory** sub-node.



Screenshot 59 - Application inventory

2. From the right panel locate the application to configure as unauthorized and under **Unauthorized on**, click **Click to configure...** link.



Screenshot 60 - Mark application as unauthorized

3. Select the scanning profile that will classify the application as High Security Vulnerability and click **Next**.

4. Review the currently affected applications screen and click **Finish** to finalize settings.

Refer to the [Applications inventory](#) section in this manual for more information on defining unauthorized applications.

Validate applications to uninstall remotely:

1. From the **Configuration** tab, select **Applications inventory ► Auto-Uninstall Validation** sub-node.

2. In the right pane, select an application to validate and click **Validate...**

3. In the **Application auto-uninstall validation** wizard click **Next** and select the computer where to test the application auto-uninstall. Click **Next**.

4. Provide the authentication details for the validation operation and click **Next**.

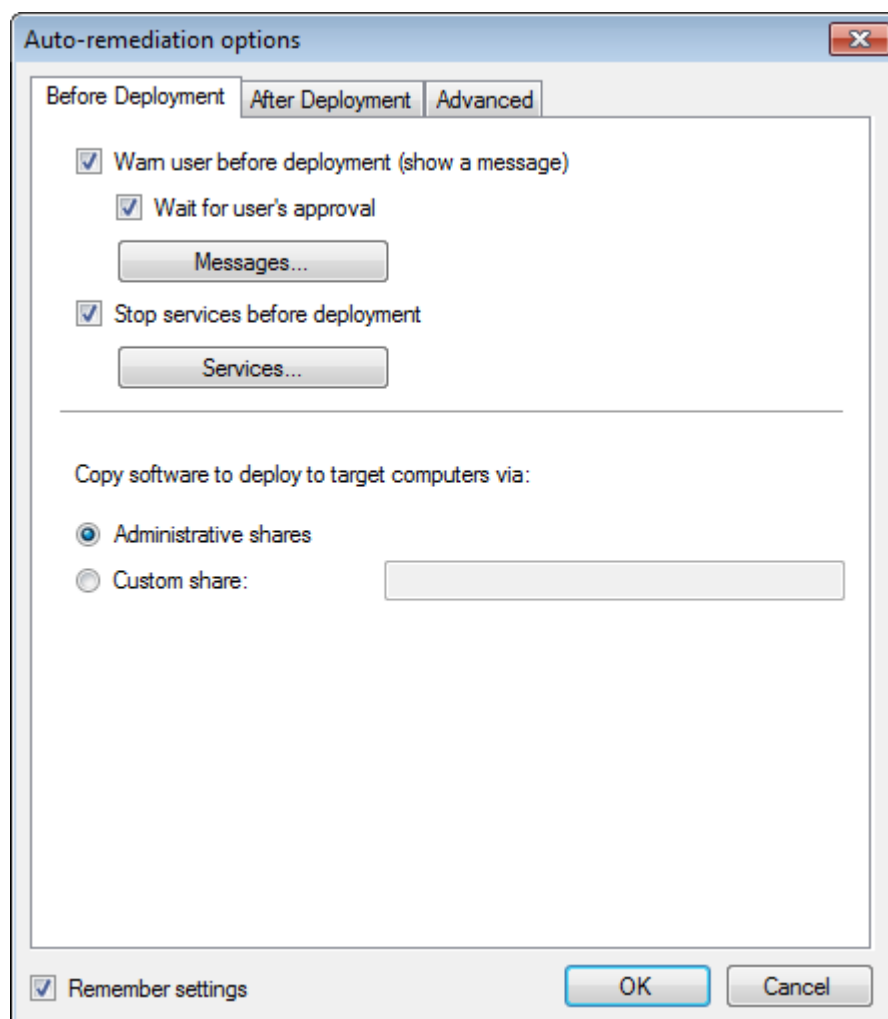
5. Review the **Auto-uninstall validation wizard** information and click **Start** to validate application auto-uninstall.

For more information on auto-uninstall validation refer to [Application auto-uninstall validation](#) in this manual.

5.2.3 Auto-remediation options

To edit the general deployment options, after a scan:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Remediate** tab ► **Remediation Center**. Select a remediation action from the right panel and click **Options**.



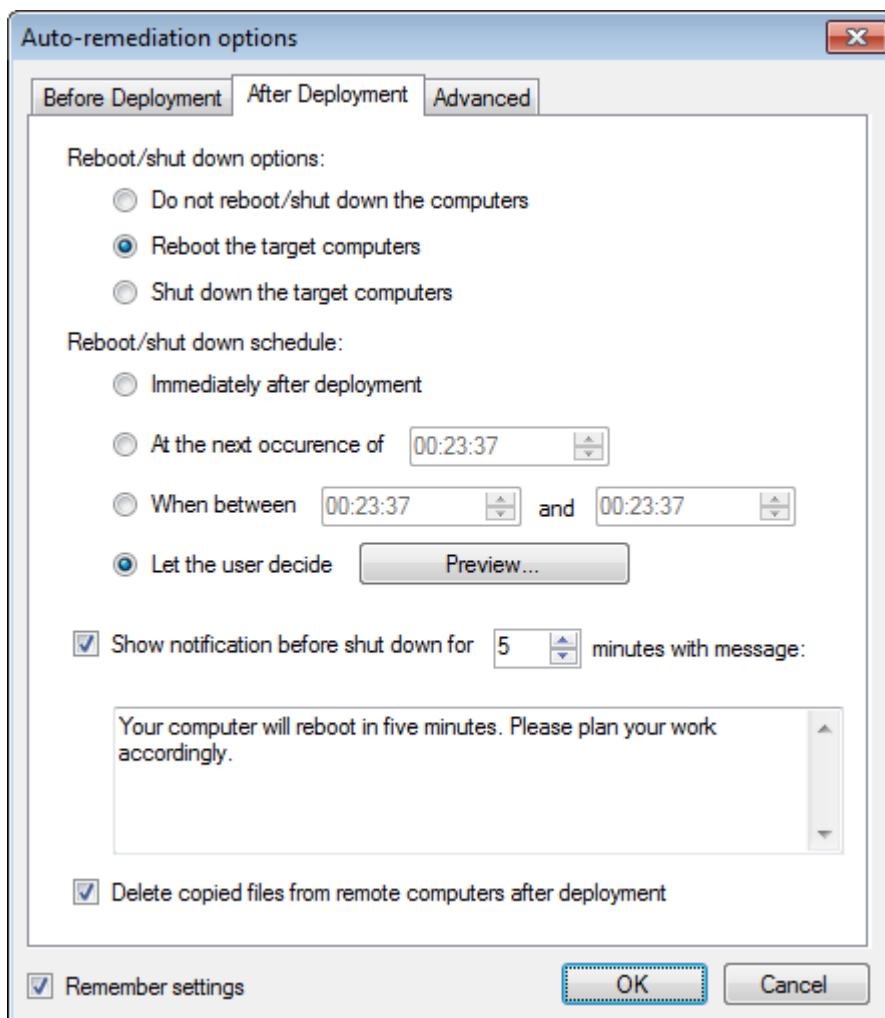
Screenshot 61 - Before deployment options

3. Configure **Before Deployment** options described below:

Table 26 - Before deployment

OPTION	DESCRIPTION
Warn user before deployment (show message)	Displays a message on the target machine to warn the user before deploying software.
Wait for user's approval	Waits for user approval before deploying software.
Messages	Click Messages... to select the end-user's computer language and define the warning message. For more information, refer to Define auto remediation messages section in this manual.
Administrative shares	Make a copy of the software on the default network shares.
Custom shares	Make a copy of the software in a custom share. Key-in the folder name in the text box.

OPTION	DESCRIPTION
Remember settings	Saves your configured settings and uses them during the next remediation job.



Screenshot 62 - After deployment options

4. Click **After Deployment** tab. Configure **After Deployment** options described below:

Table 27 - After deployment

OPTION	DESCRIPTION
Do not reboot/shutdown the computer	Select this option to leave scan target(s) turned on after remediating vulnerabilities.
Reboot the target computers	Reboots the computers after remediating vulnerabilities.
Shut down the target computers	Target machine will shut down after deploying software.
Immediately after deployment	Reboots/shuts down computers immediately after remediating vulnerabilities.
At the next occurrence of	Specify the time when the computers reboot/shut down.
When between	This option enables you to specify two time values. If the remediation job is completed between the specified times, the computer(s) will reboot/shut down immediately. Otherwise, the reboot/shut down operation is postponed until the next entrance into the specified time interval.
Let the user decide	Click Preview... to view a screenshot of the dialog in the user manual. This dialog opens on the end-user's computer after remediating vulnerabilities. For more information, refer to End-user reboot and shut down options section in this manual.

OPTION	DESCRIPTION
Show notification before shut down for	Shows a custom message on the end user's computer for a specified number of minutes before reboot/shut down.
Delete copied files from remote computers after deployment	Deletes the downloaded patches / service packs after they are deployed.
Remember settings	Saves your configured settings and uses them during the next remediation job.

Auto-remediation options

Before Deployment | After Deployment | **Advanced**

Number of deployment threads: (max 10)
 WARNING: Deploying with more than 5 threads may render the UI unresponsive until the deployment operation is complete.

Deployment timeout (seconds):

☒ Deploy patches under the following administrative account
 (domain\user or user@FQDN format):

Account name:
 Password:

Note: Only select this option if you want to run the installation packages on the target computers under an account other than the Local System account. If you need to select this option, make sure that the specified account has the Log on as service privilege on the target computers.

☒ Remember settings

OK Cancel

Screenshot 63 - Advanced deployment options

4. (Optional) Select **Advanced** tab. Configure the options described below:

Table 28 - Advanced deployment options

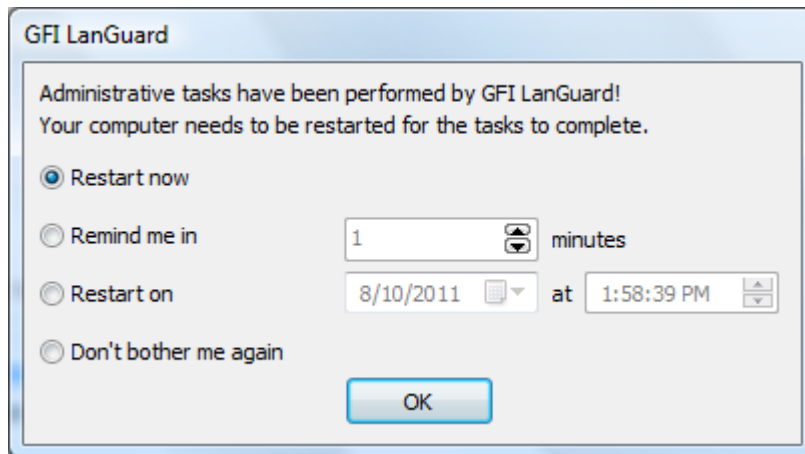
OPTION	DESCRIPTION
Number of deployment threads	Key-in the number of threads to use when deploying software. The number of threads determines the number of simultaneous deployment.
Deploy patches under the following administrative account.	Select this option to use a custom administrative account to log and deploy patches on target machines. Key-in a valid username and password. The account selected must have Log-on as service privilege on the target computers. For more information on how to configure an account with log-on as service privilege, refer to: http://technet.microsoft.com/en-us/library/cc739424(WS.10).aspx

OPTION	DESCRIPTION
Deploy patches with their original names	Deploy patches on target machines using the original patches name. If this option is not selected GFI LanGuard will give a unique name for each patch.

6. Click **OK** to apply changes.

5.2.4 End-user reboot and shut down options

When configuring **After Deployment** settings, in **Auto-remediation options**, you can configure GFI LanGuard to notify and let the user decide when to reboot or shut down the computer after completing an administrative task. The below dialog opens on the user's computer and enables him/her to select one of the following options:



Screenshot 64 - Reboot/shut down options

The table below describes the available options:

Table 29 - Advanced deployment options

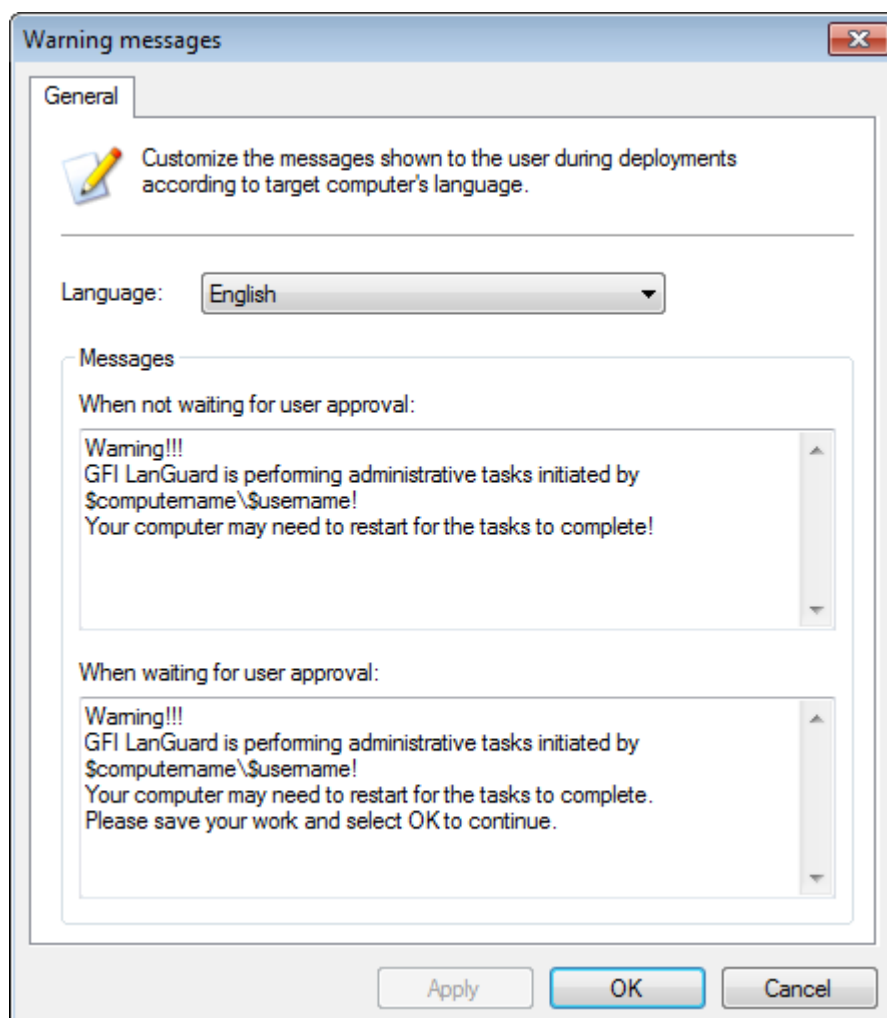
OPTION	DESCRIPTION
Restart now	Reboots/shuts down the computer immediately after completing an administrative task.
Remind me in	Specify a time interval (in minutes), when to remind the end-user.
Restart on	Specify the date and time when the machine reboots/shuts down.
Don't bother me again	The user is not prompted again.

5.2.5 Define auto-remediation messages

GFI LanGuard allows you to specify warning messages for auto remediation operations. You can customize predefined messages and set the language according to the target computer's language.

To specify warning messages:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Remediate** tab ► **Remediation Center**. Select a remediation action from the right panel and click **Options**.
3. From **Before Deployment** tab, select **Warn user before deployment (show a message)**.
4. Click **Messages...**



Screenshot 65 - Warning messages

5. Specify the options described below:

Table 30 - Warning messages

OPTION	DESCRIPTION
Language	Select the language the message language.
When not waiting for user approval	Use or customize the pre defined message that launches on the end-user's computer when GFI LanGuard is not waiting for approval.
When waiting for user approval	Use or customize the pre defined message that launches on the end-user's computer when GFI LanGuard is waiting for approval.

5.2.6 Agent auto-remediation

In an agent-based environment, automatic remediation options can be set per every deployed agent. This enables you to configure every agent with specific auto-remediation options to suit your requirements.



For information about configuring agent auto-remediation, refer to [Customizing agents](#) section in this manual.

5.3 Remediation center

Apart from automatically downloading patches and service packs, GFI LanGuard can also deploy these updates network-wide as well as recall any patches that were deployed.



While an infrequent occurrence, patches may be recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates such as conflict issues with present software or hardware. Examples of updates recalled by the manufacturer include patches MS03-045 and MS03-047 for Exchange that were released by Microsoft on October 15, 2006.

Both patch deployment and patch rollback operations are managed by an agent service that manages all file transfers between GFI LanGuard and remote targets. This service is installed automatically on the remote target computer during the patch deployment process.

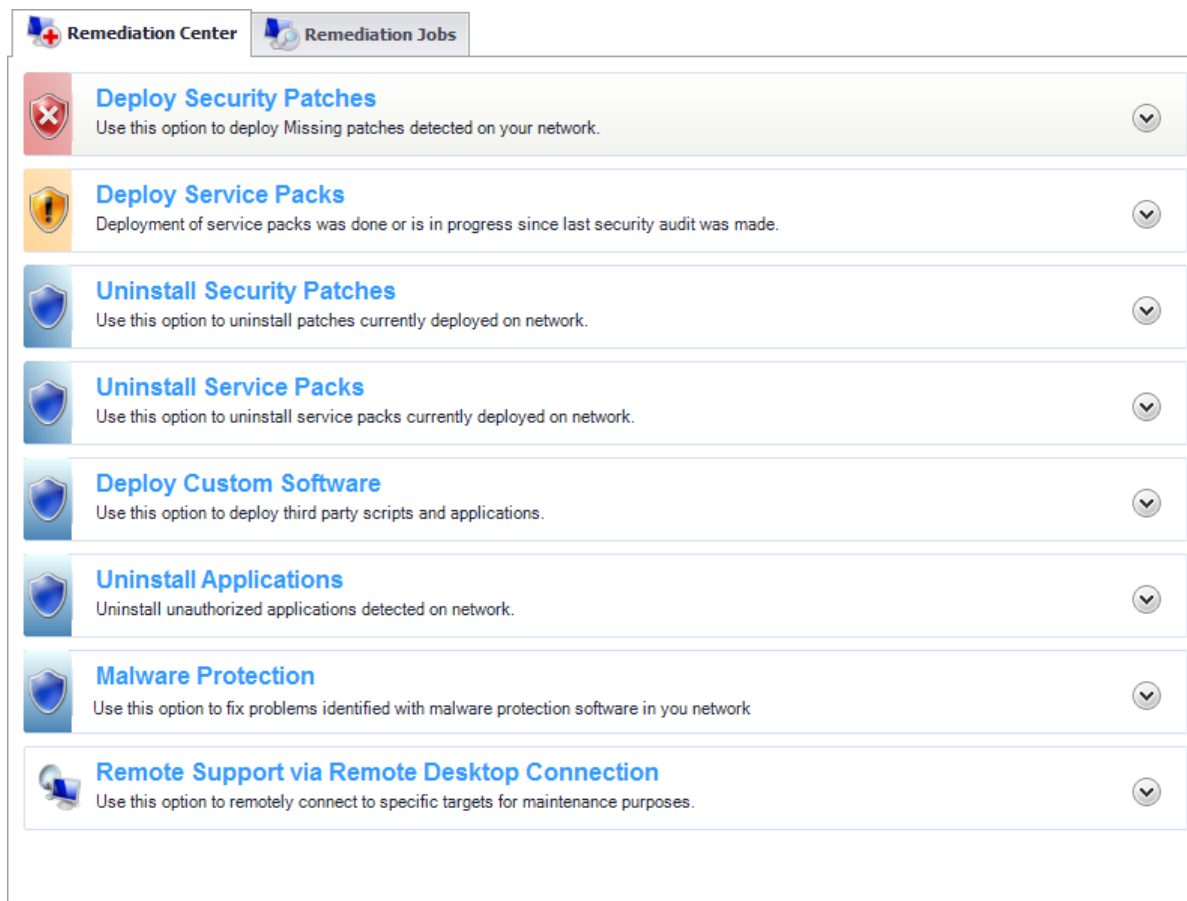
The **Remediation Center** enables you to fix security issues found during a network scan by deploying or uninstalling applications from target machines. To access the **Remediation Center**, select **Remediate** tab ► **Remediation Center**.



To deploy missing patches on scan targets, ensure that GFI LanGuard is running under an account that has administrative privileges.

Important notes

1. Ensure that the NetBIOS service is enabled on the remote target computer. For more information on how to enable NetBIOS, refer to the [Enabling NetBIOS on a network computer](#) section in this manual.
2. A complete list of Microsoft products for which GFI LanGuard can download and deploy patches is available at <http://kbase.gfi.com/showarticle.asp?id=KBID001820>.
3. Non-Microsoft software update patches supported by GFI LanGuard is available at <http://www.gfi.com/lannetscan/3pfullreport.htm>.
4. GFI LanGuard can be set to automatically download missing patches and service packs discovered during a network security scan. For more information, refer to the [Configuring Microsoft updates](#) section in this manual.



Screenshot 66 - Remediation center

5. From the left panel, expand and locate a computer or a domain to perform remediation actions. The available remediation actions are described below:

Table 31 - Remediation actions

ACTION	DESCRIPTION
Deploy Security Patches	Deploy missing patches discovered when auditing target computers. For more information on how to deploy patches, refer to Deploy security patches and service packs section in this manual.
Deploy Service Packs	Deploy missing service packs found when auditing target computers. For more information on how to deploy, service packs refer to Deploy security patches and service packs section in this manual.
Uninstall Software Patches	Uninstall software patches from target computers. For more information on how to uninstall, software patches refer to Uninstall software patches and service packs section in this manual.
Uninstall Service Packs	Uninstall service packs from target computers. For more information on how to uninstall, service packs refer to Uninstall software patches and service packs section in this manual.
Deploy Custom Software	Deploy custom applications and scripts on target computers. For more information on how to deploy custom software, refer to Deploy custom software section in this manual.
Uninstall Applications	Uninstall applications from target computers. For more information on how to manually uninstall applications from target computers, refer to Uninstall custom applications section in this manual.
Malware Protection	Perform Malware protection actions on target computers. For more information on how to perform Malware protection actions, refer to Malware protection actions section in this manual.

ACTION	DESCRIPTION
Remote Support via Remote Desktop Connection	Connect to a target machine and perform administrative tasks using remote desktop connection. For more information on how to connect remotely to a target machine, refer to Using remote support section in this manual.



You can use GFI LanGuard filtering option to locate a machine. For more information, refer to [Display results](#) section in this manual

5.4 Deploy security patches and service packs

To deploy missing security patches and service packs on specific computers:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Select **Remediate** tab ► **Remediation Center**.
3. From the left panel, select the computer or domain where you want to perform the remediation action.
4. From the right panel, click on **Deploy Security Patches** or **Deploy Service Packs**.

1 Specify patches to deploy

☒		Bulletin	Severity	Date posted	Title	Applie...
☒		Not Available	Critical	2011-07-12	Windows Malicious Software Removal Tool - July 2011 (KB890...	Windows
☒		MS11-054	Important	2011-07-12	Security Update for Windows 7 (KB2555917)	Windows
☒		MS11-053	Critical	2011-07-12	Security Update for Windows 7 (KB2532531)	Windows
☒		MS11-055	Critical	2011-07-12	Security Update for Windows 7 (KB2555917)	Windows
Count=50						

Screenshot 67 - Select the updates to deploy

5. From the list of missing patches/service packs, select the updates to deploy. Right-click on the list to access **Check/Uncheck all** options.

2 Specify computers where to deploy each patch

☒		Computer name	Language	Operating system
☒		TEMP	English	Windows 7
☒		W703	English	Windows 7
Count=2				

Screenshot 68 - Deploying missing patches on selected computers

6. From the list of target computers, select the target computers where to deploy patches/service packs. Right-click on list to access **Check/Uncheck all** options.

Screenshot 69 - Deploy patches

7. Select the preferred launch deployment option.

- » Choose **Deploy on** to schedule patch/service pack deployment to a later date/time. Specify date and time.
- » Choose **Deploy immediately** to start the deployment immediately. Click Remediate Now.

8. Configure the authentication credentials to use; select between:

- » **Currently logged user**
- » **Alternative credentials**
- » **A null session**

9. Follow any on-screen instructions (if applicable).

5.4.1 Patch deployment warning message

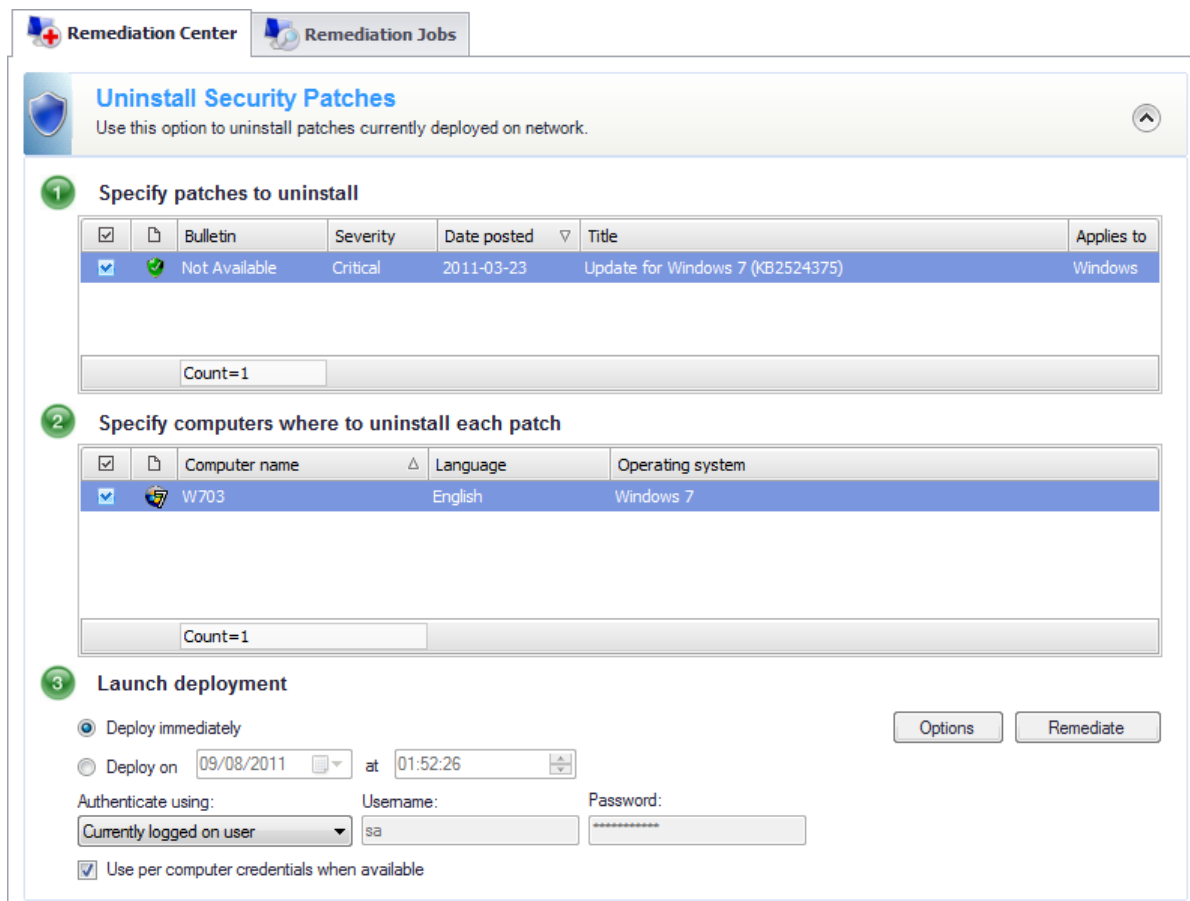
Deploying patches triggers a warning message on targets computer to inform users about the installation process.

Depending on the patch deployment configuration, one of two messages is shown. These messages are fully customizable, enabling you to display any information suitable to your requirements. For information, refer to [Auto-remediation options](#) section in this manual.

5.5 Uninstall software patches and service packs

To roll back deployed patches and service packs:

1. Select **Remediate** tab ► **Remediation Center**.
2. From the left panel, select the computer or domain where you want to perform the remediation action.
3. From the right panel select **Uninstall Security Patches** or **Uninstall Service Packs**.



Screenshot 70 - Uninstall security patches

4. Select the patches or service packs to uninstall from selected targets.
5. (Optional) Select **Deploy on**, configure the date, and time when you want to uninstall the selected application/patch.
6. Configure the authentication credentials to use, select between:
 - » **Currently logged user**
 - » **Alternative credentials**
 - » **A null session**
7. Click **Remediate Now** to start the uninstall process.

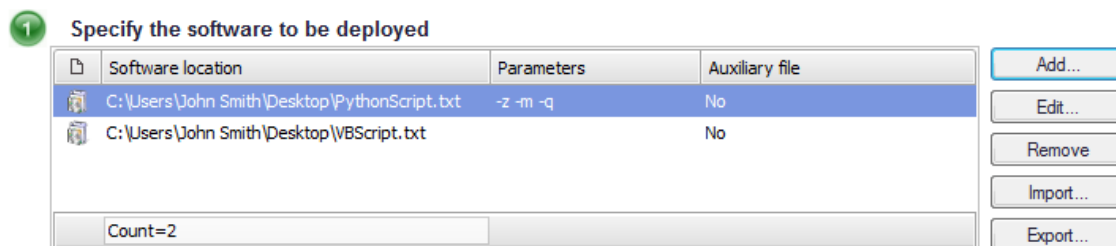
5.6 Deploy custom software

Apart from security updates and patches, GFI LanGuard also enables you to remotely deploy third party or custom software network-wide. Software that can be remotely deployed includes:

- » **Security applications** such as anti-virus/anti-spyware solutions and software firewalls
- » **Third party software updates and patches** such as anti-virus/anti-spyware signature file updates
- » **Custom code** such as scripts and batch-files
- » **Desktop applications** such as Microsoft Office 2007 and more.

To specify which software to deploy:

1. Click on **Remediate** tab ► **Remediation Center**.
2. Click **Deploy Custom Software**.

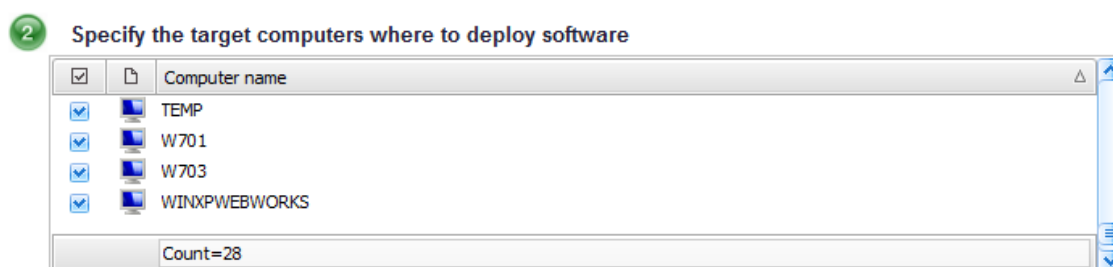


Screenshot 71 - List of software to be deployed

3. Use the options described in Table 32 below to add the applications to deploy:

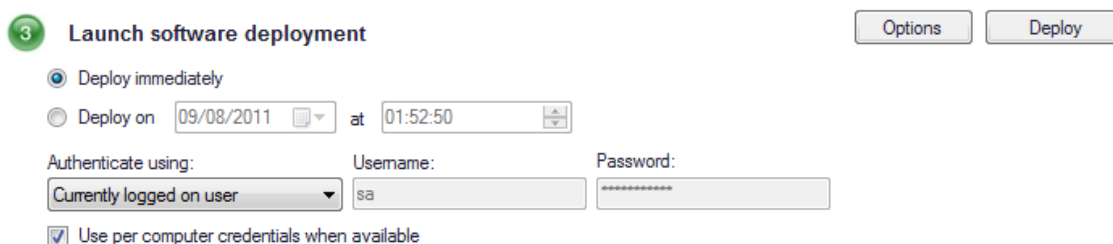
Table 32 - Options available in Deploy Custom Software

OPTION	DESCRIPTION
Add	Click this button to launch the Add custom software dialog. This dialog enables you to add an application to the list and if required configure parameters.
Edit	Select an application and click this button to launch the Add custom software dialog. This dialog enables you to modify the existing installation parameters.
Remove	Select an application from the list and click this button to remove the application.
Import	Click this button to import the applications parameters from an XML file.
Export	Click this button to export the applications parameters to XML file.



Screenshot 72 - Target computers for software deployment

4. Select the target computers where to deploy software. Right-click on a target computer to select between **Check all** / **Uncheck all** options.



Screenshot 73 - Launch deployment options

6. Configure the authentication credentials to use. Select between:

- » **Currently logged user**
- » **Alternative credentials**
- » **A null session**

7. Select the preferred launch deployment option. Table 33 below describes the available options:

Table 33 - Launch deployment options

OPTION	DESCRIPTION
Deploy on	Schedule patch / service pack deployment to a later date / time.
Remediate now	Start deployment immediately.

8. To view the deployment progress, click **Remediation Jobs** from the right panel. For more information, refer to [Remediation Jobs](#) section in this manual.

5.7 Uninstall custom applications

Using this feature, you can control the installed applications, on which computers, and uninstall any unauthorized applications present on network computers.

To uninstall applications:

1. Select **Remediate** tab ► **Remediation Center** and click **Uninstall Applications**.

Uninstall Applications
Uninstall unauthorized applications detected on network.

1 Specify which applications to uninstall to which computers

☒	Application name	Version	Publisher	Uninstall string	User
☒	Adobe Flash Player 10 ActiveX	10.1.82.76	Adobe Systems Incorporated	"C:\Windows\system32\Mac...	
☒	Alchemy Catalyst 9.0	9.00.0000	Alchemy Software Develop...	MsIExec.exe /quiet /noresta...	
☒	Alchemy Publisher 3.0	3.00.0000	Alchemy Software Develop...	MsIExec.exe /quiet /noresta...	

Count=25

2 Specify the target computers where to uninstall applications

☒	Computer name	Operating system
☒	TEMP	Windows 7

Count=1

3 Launch uninstall

☒ Uninstall immediately
☐ Uninstall on 09/08/2011 at 01:57:00

Authenticate using: Currently logged on user Username: sa Password: *****

☒ Use per computer credentials when available

Options Uninstall

Screenshot 74 - Uninstall applications

2. Select the applications to uninstall and the computers to uninstall from.



The list of applications displayed relies on the unauthorized applications set up for the scanning profile in use. For more information on how to set up and validate applications to uninstall refer to the [Applications inventory](#) and [Application auto-uninstall validation](#) sections in this manual.

3. Configure the authentication credentials to use. Select from:

- » **Currently logged user**
- » **Alternative credentials**
- » **A null session**

4. Select the preferred uninstall option described in Table 34 below:

Table 34 - Uninstall options

OPTION	DESCRIPTION
Uninstall on	Schedule patch / service pack uninstallation to a later date / time.
Uninstall immediately	Uninstall the selected applications immediately.

5. Click **Uninstall Now** to uninstall applications based on your configuration.

6. To view the un-installation progress, click **Remediation Jobs** from the right panel. For more information on Remediation Jobs, refer to [Remediation Jobs](#) section in this manual.

5.8 Malware protection actions

Use the **Malware Protection** section to remediate vulnerabilities related to malware protection identified on target computers. Amongst others, this section enables you to scan target machines for spyware, viruses and enable local firewall.



To scan a machine for viruses and spyware, the target machine must have anti-virus and anti-spyware installed.

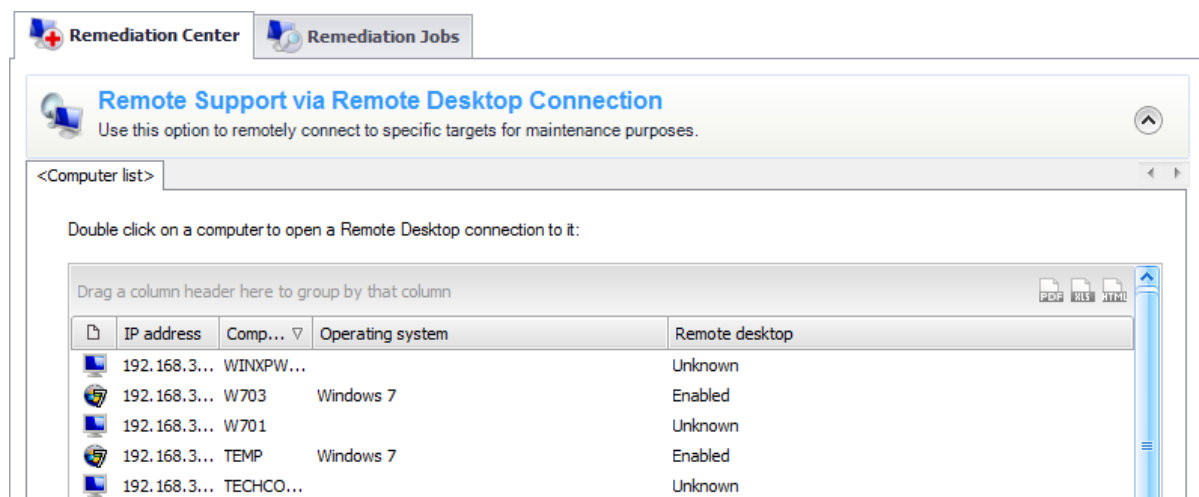
Screenshot 75 - Malware protection

To remediate malware protection vulnerabilities:

1. Select **Remediate** tab ► **Remediation Center** and click **Malware Protection**.
2. Select the action/computer combination.
3. Configure the authentication credentials to use, select from:
 - » **Currently logged user**
 - » **Alternative credentials**
 - » **A null session**
4. Select **Deploy immediately** to immediately uninstall any applications selected or provide a date/time combination in the **Deploy on** field.
5. Click **Remediate Now** to uninstall applications based on your configuration.
6. To view the action progress, click **Remediation Jobs** from the right panel. For more information on Remediation Jobs, refer to [Remediation Jobs](#) section in this manual.

5.9 Using remote support

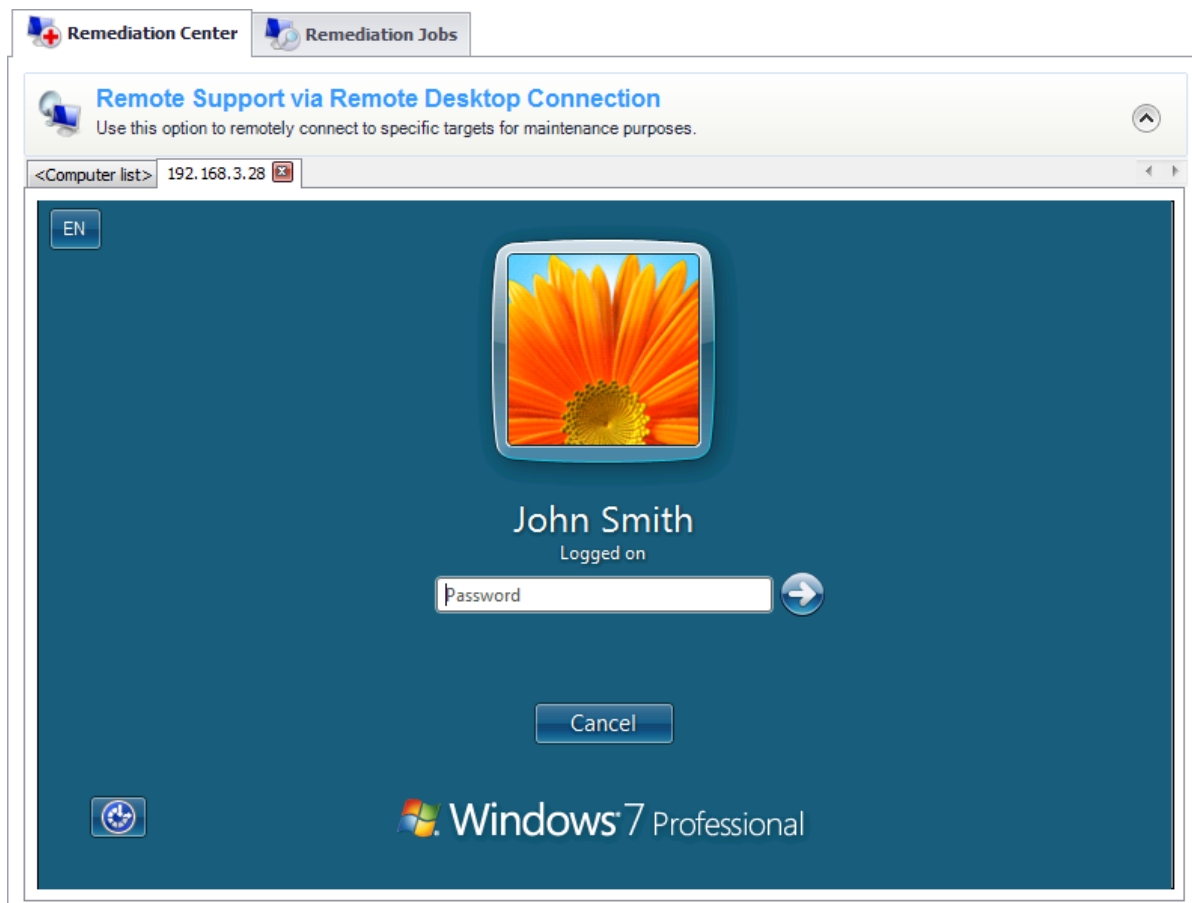
Through Remote Support, you can control remote computers using Terminal Services and Remote Desktop Protocol. Remote Support enables you to install missing patches, service packs and custom software through a remote connection.



Screenshot 76 - Remote desktop connection

To connect remotely to a target machine:

1. Click **Remediate** tab and from the left panel select a computer or domain/workgroup.
2. Expand **Remote Support via Remote Desktop Connection** from the right panel.
3. Depending on your selection, the list contains the available computers that allow remote desktop connection.
4. Double click a machine from the list to connect.



Screenshot 77 - Remote desktop connection



To disconnect a machine, select **Remediation Center ► Remote Support via...**, right-click a machine from the list and select **Disconnect**.

5.10 Remediation Jobs

The **Remediation Jobs** section enables you to monitor the remediation actions in progress. To open the **Remediation Jobs**, click **Remediate** tab ► **Remediation Jobs**.



Select a computer from the left panel to view the progress for that computer.

Remediation Center
 Remediation Jobs

Remediation jobs for selected computers:

Drag a column header here to group by that column

PDF XLS HTML

	Status	Remediation Type	Scheduled on	Started On	Ended On
	Complete wit...	Security Service Packs D...	04/08/2011 23:22:51	04/08/2011 23:22:59	04/08/2011 23:42:51
	Complete wit...	Security Service Packs D...	04/08/2011 23:22:42	04/08/2011 23:22:51	05/08/2011 00:04:57
	Complete wit...	Security Service Packs D...	04/08/2011 23:21:59	04/08/2011 23:22:09	04/08/2011 23:50:39

Count=3

Note: Bold remediation jobs indicate that the job was started after the last audit. The vulnerability level will be updated when the next audit is started.

Remediation job details:

Downloads

TEMP (Failed: PatchAgent is performing another remediation session on the target computer)

Progress details

Microsoft SQL Server 2005 Express Edition Service Pack 4 (KB2463332): failed

Windows 7 Service Pack 1 (KB976932): failed

Windows 7 Service Pack 1 (KB976932): failed

W703 (Completed)

Progress details

Windows 7 Service Pack 1 (KB976932): completed

Windows 7 Service Pack 1 (KB976932): completed

Auto-remediation status:

No agents with auto-remediation enabled.

No scheduled scans with auto-remediation enabled.

Screenshot 78 - Remediation jobs

To stop a deployment action, right-click a remediation job entry and select Cancel selected deployment.

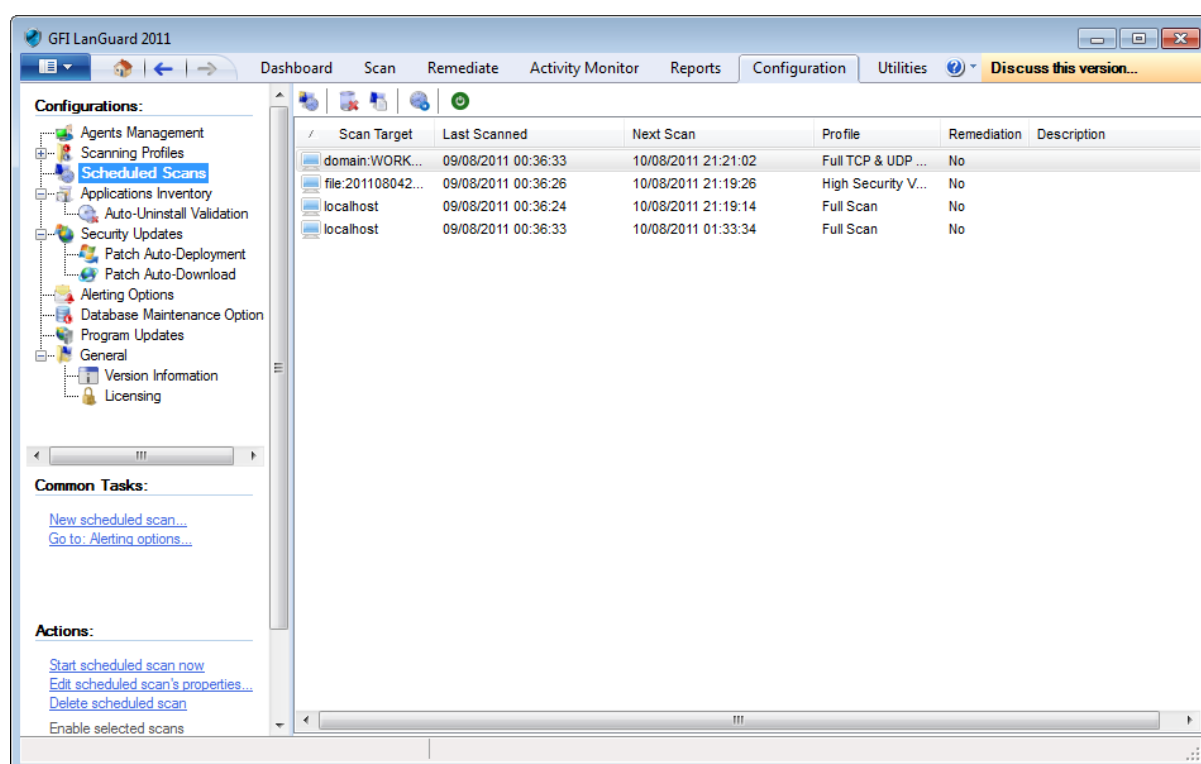
6 Configuring GFI LanGuard

6.1 Introduction

GFI LanGuard enables you to run vulnerability scans straight out of the box - using the default settings configured prior to shipping. If required you can also customize these settings to suit any particular vulnerability management requirements that your organization might need. You can customize and configure various aspects of GFI LanGuard including scan schedules, vulnerability checks, scan filters and scan profiles.

6.2 Scheduled Scans

Scheduled scans enable you to automate the process of performing regular scans, auditing and remediation procedures.



Screenshot 79 - Scheduled scans

6.2.1 Reviewing, editing or deleting scan schedules

Scan schedules can be reviewed, edited, or deleted from Configuration tab ► Scheduled Scans node.



Screenshot 80 - Scheduled scan toolbar

All scans are listed in the review page together with the relevant information. Use the scheduled scan toolbar to perform the actions described in Table 35 below:

Table 35 - Options to manage scanning profiles

COMPLETE/COMBINATION SCANS SCANNING PROFILES	
	Add new scan - Display the New scheduled scan wizard and create a new scheduled scan.
	Delete - Use this button to delete the selected scheduled scan.

COMPLETE/COMBINATION SCANS SCANNING PROFILES

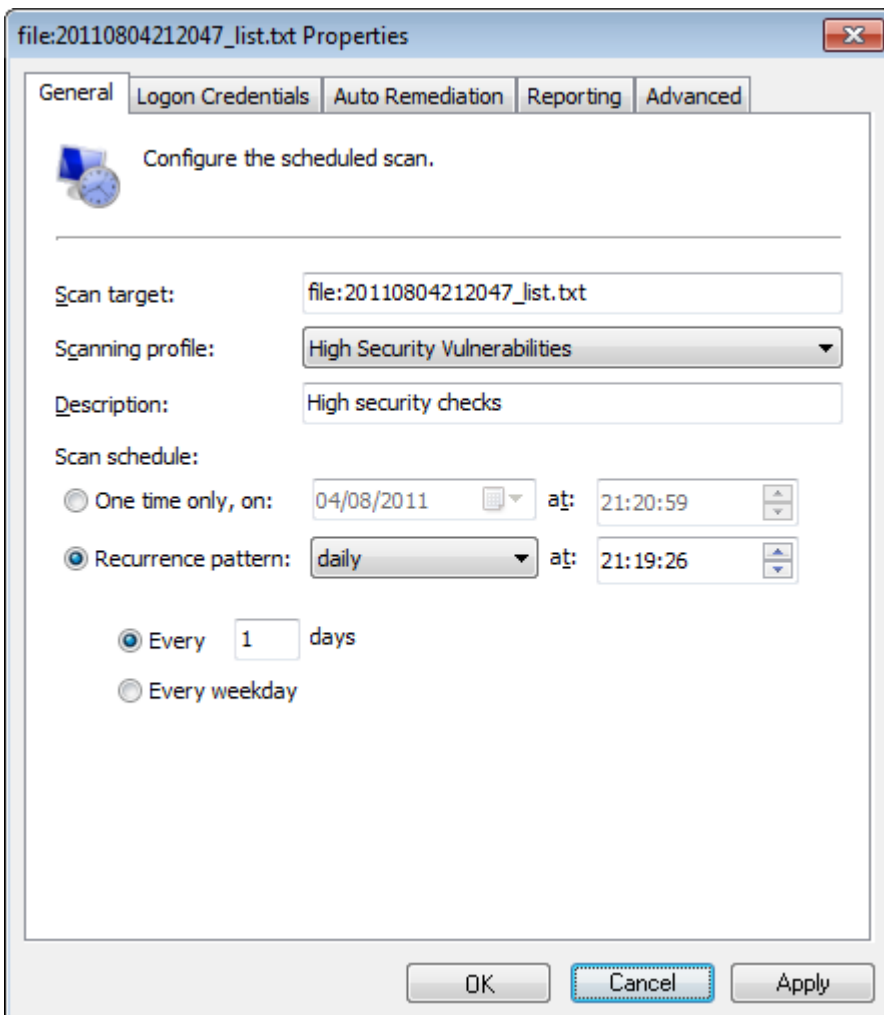
	Properties - Review and edit the properties of the selected scan.
	Enable/Disable - Toggle the status of the selected scan between enabled and disabled. This enables you to activate/suspend a scanning schedule without deleting the scheduled scan.
	Scan now - Trigger the selected scheduled scan. This button overrides the scheduled scan date/time settings and executes an immediate scan.

6.2.2 Scheduled scan properties

The scheduled scan properties page enables you to configure all the parameters of the scheduled scans.

To use the scheduled scan properties tab:

1. Go to **Configuration** tab ► **Scheduled Scans**.
2. Select the scheduled scan and click the **Scheduled Scan Properties** .



file:20110804212047_list.txt Properties

General Logon Credentials Auto Remediation Reporting Advanced

 Configure the scheduled scan.

Scan target: file:20110804212047_list.txt

Scanning profile: High Security Vulnerabilities

Description: High security checks

Scan schedule:

☐ One time only, on: 04/08/2011 at: 21:20:59

☒ Recurrence pattern: daily at: 21:19:26

☒ Every 1 days

☐ Every weekday

OK Cancel Apply

Screenshot 81 - Scheduled Scan properties

3. Modify the options described below:

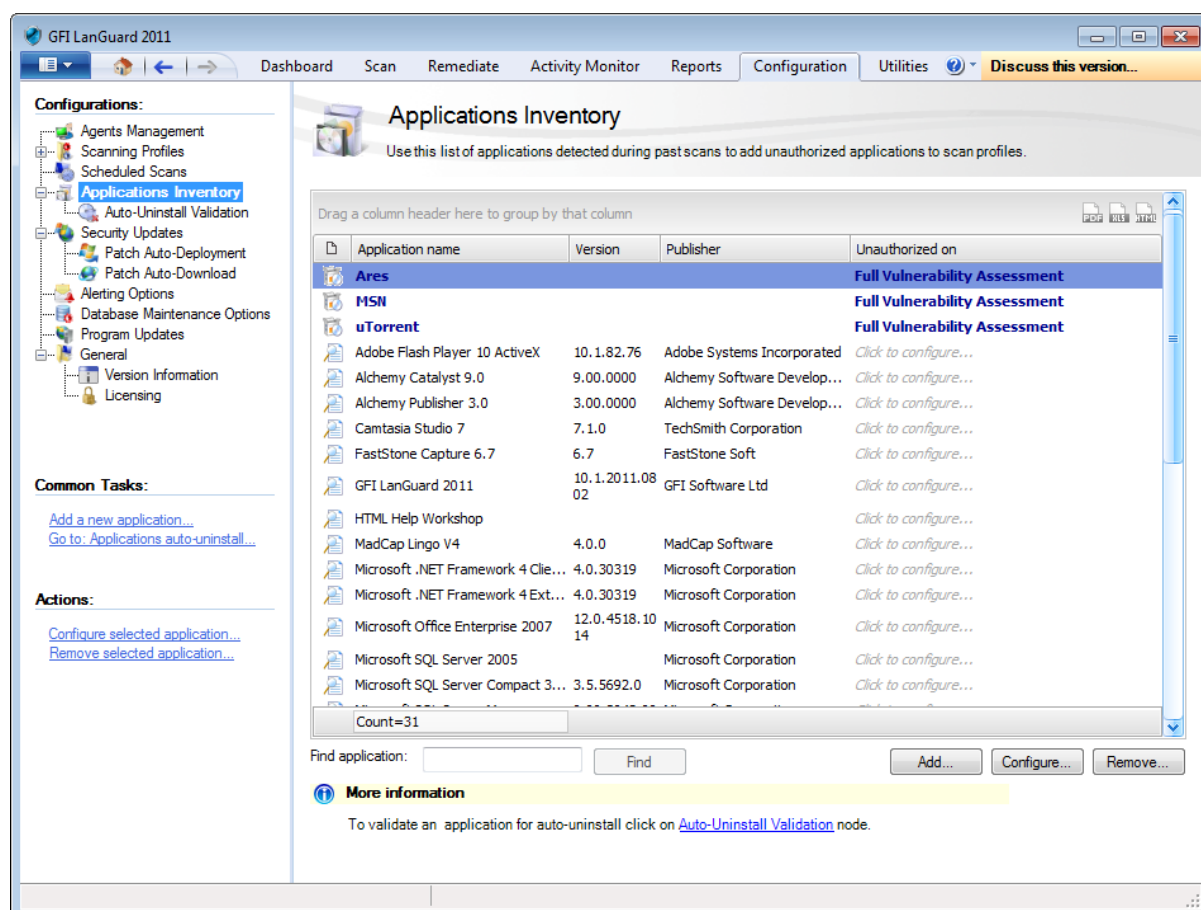
Table 36 -Schedule scan properties

TAB NAME	DESCRIPTION
General	Make changes to scan target setting, type of scanning profile and scan frequency.
Logon Credentials	Use this tab to specify logon credentials used when scanning the specified target.
Auto-remediation	Use this tab to configure the remediation options applicable to the scan being configured. This includes downloading and installing missing patches and service packs and unauthorized software un-installation.
Reporting	Configure reporting options used for the selected scheduled scan.
Advanced	Use this tab to specify whether GFI LanGuard should wait for offline computers to connect to the network. This enables GFI LanGuard to postpone the scan on these machines and keep track of targets pending a scan. For example, laptops or other mobile devices, that are not connected to the network. As soon as these are connected, scanning will start.

4. Click OK to finalize your configuration.

6.3 Applications inventory

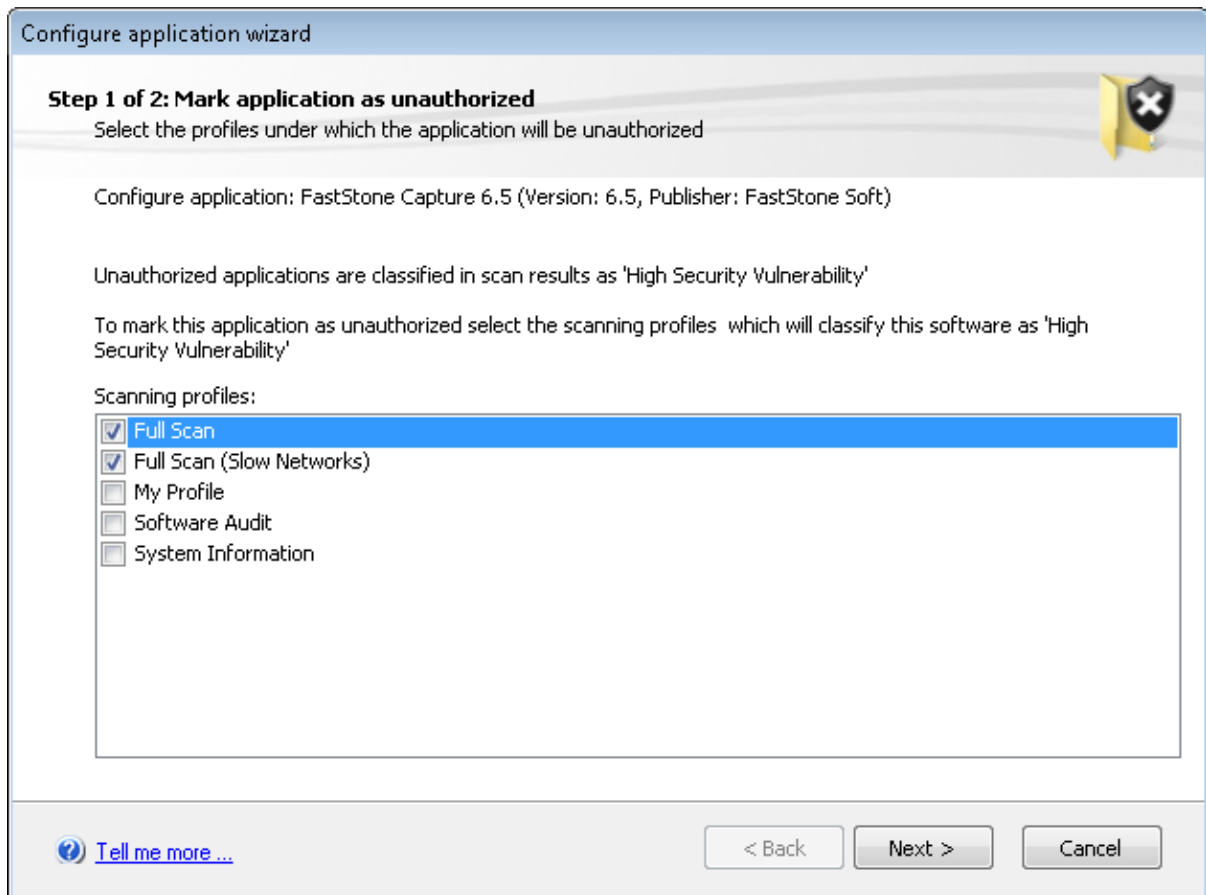
GFI LanGuard applications inventory provides a list of all applications detected during past scans. The list is used to specify unauthorized applications. You can also manually add applications to the list. You can do this by specifying the entire name as well as a partial name, specify generic names or part of an application name. GFI LanGuard automatically scans the list of applications and detects partial names.



Screenshot 82 - Configuring Applications inventory

To indicate an application as unauthorized:

1. Click on **Configuration** tab ► **Applications inventory** sub-node.
2. From the list of applications detected on the right, double click the application to set as unauthorized.



Screenshot 83 - Unauthorized application - scanning profile

3. Select the scanning profile for which this application will be set as unauthorized and click **Next**.
4. GFI LanGuard can associate partial names with entries already in the list. As a result, the system will prompt you to confirm whether to apply the same changes also to applications partially have the same name.
5. Click **Finish** to finalize settings.

6.3.1 Adding a new unauthorized application

To add a new application manually without using the inventory:

1. Click **Configuration** tab ► **Applications inventory** sub-node.
2. From **Common Tasks**, click **Add a new application...**
3. In the welcome screen, click **Next**.

Add unauthorized application wizard

Step 1 of 4: Specify application details
Specify a generic application name and optional details such as publisher and version

Specify a complete or partial application name by which this application can be identified:

Application name

Note: Partial application names are accepted.

Optionally you can provide the following details:

Version Number

Publisher

[Tell me more ...](#)

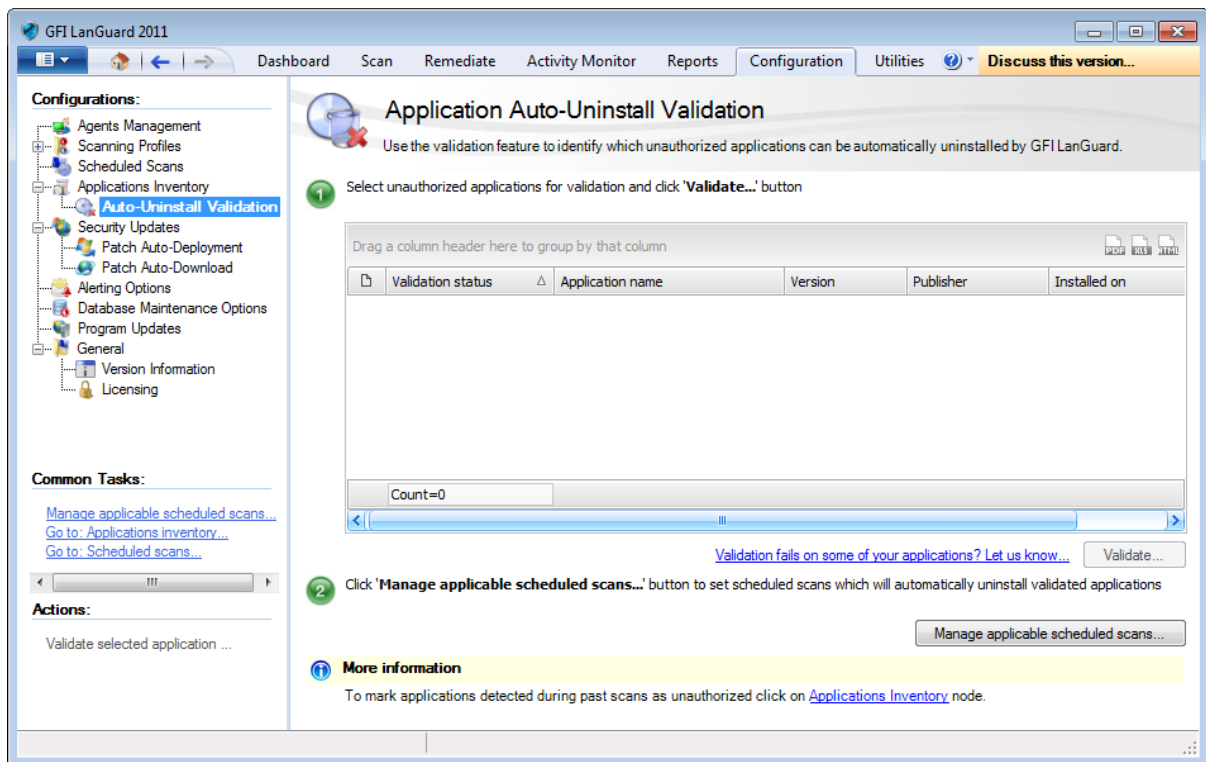
Screenshot 84 - Applications inventory wizard

4. Specify application name. Optionally provide the version number and publisher name. Click **Next**.
5. Select the scanning profiles that will detect unauthorized applications (Example: **Full Scan**) and click **Next**.
6. Specify whether changes made will effect applications, which have partial/full name match. Click **Next** to continue.
7. Review **Add application wizard** information and click **Finish** to finalize configuration.

6.3.2 Application auto-uninstall

Application auto-uninstall entails that applications marked as unauthorized for specific scanning profiles are first validated for a successful uninstall on a test machine. Subsequently a scheduled scan based on the scanning profile for which the application is marked as unauthorized, is configured to auto-uninstall applications.

Application auto-uninstall validation



Screenshot 85 - Application auto-uninstall validation

Application auto-uninstall validation enables you to validate the uninstallation procedure for the applications which are to be automatically uninstalled by GFI LanGuard. This is a requirement prior to the actual uninstallation process and no applications are un-installed during scans unless verified.



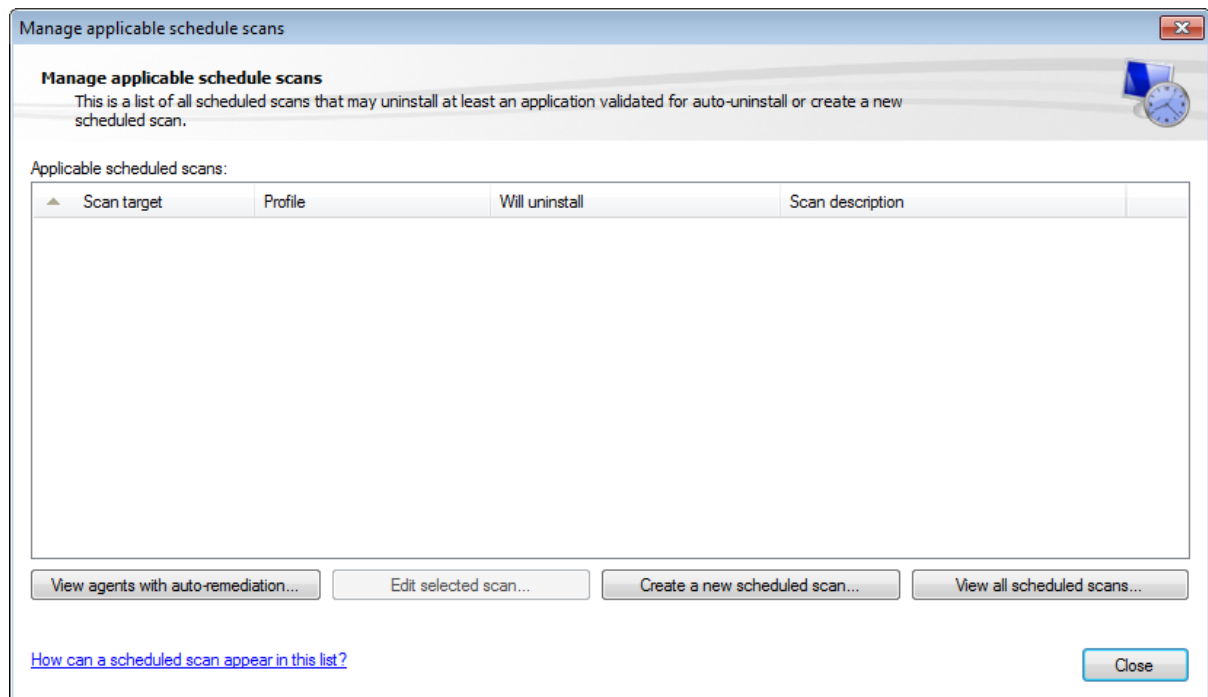
For more information on how to mark applications as unauthorized and therefore enable their uninstallation, refer to [Applications inventory section in this manual](#).

1. Click **Configuration** tab ► **Applications Inventory** ► **Auto-Uninstall Validation**
2. From the right pane, select an application to validate and click **Validate...**
3. In the Application auto-uninstall validation wizard, click **Next**.
4. Select the computer where to test the application auto-uninstall and click **Next**.
5. Provide the authentication details for the validation operation and click **Next**.
6. Review the **Auto-uninstall validation wizard** information and click **Start**.

Managing scheduled scans

The **Manage applicable scheduled scans** button enables you to review or edit scheduled scans, which will perform the validated applications auto install. To manage a scheduled scan:

1. From the **Auto-Uninstall validation** pane, click **Manage applicable scheduled scans....**



Screenshot 86 - Manage applicable schedule scans

2. From, **Manage applicable schedule scans** dialog, click one of the options described in Table 37 below:

Table 37 - Manage applicable schedule scans

OPTION	DESCRIPTION
Edit selected scan...	Modify the selected schedule scan. For more information on how to edit an existing scheduled scan, refer to Scheduled Scans section in this manual.
Create a new scheduled scan...	Add a new scheduled scan using the new scheduled scan wizard. For more information on how to set up a new scheduled scan, refer to Setting up a scheduled scan section in this manual.
View all scheduled scans...	Manage scheduled scans. For more information on how to edit an existing scheduled scan, refer to Scheduled Scans section in this manual.

6.4 Configuring security updates

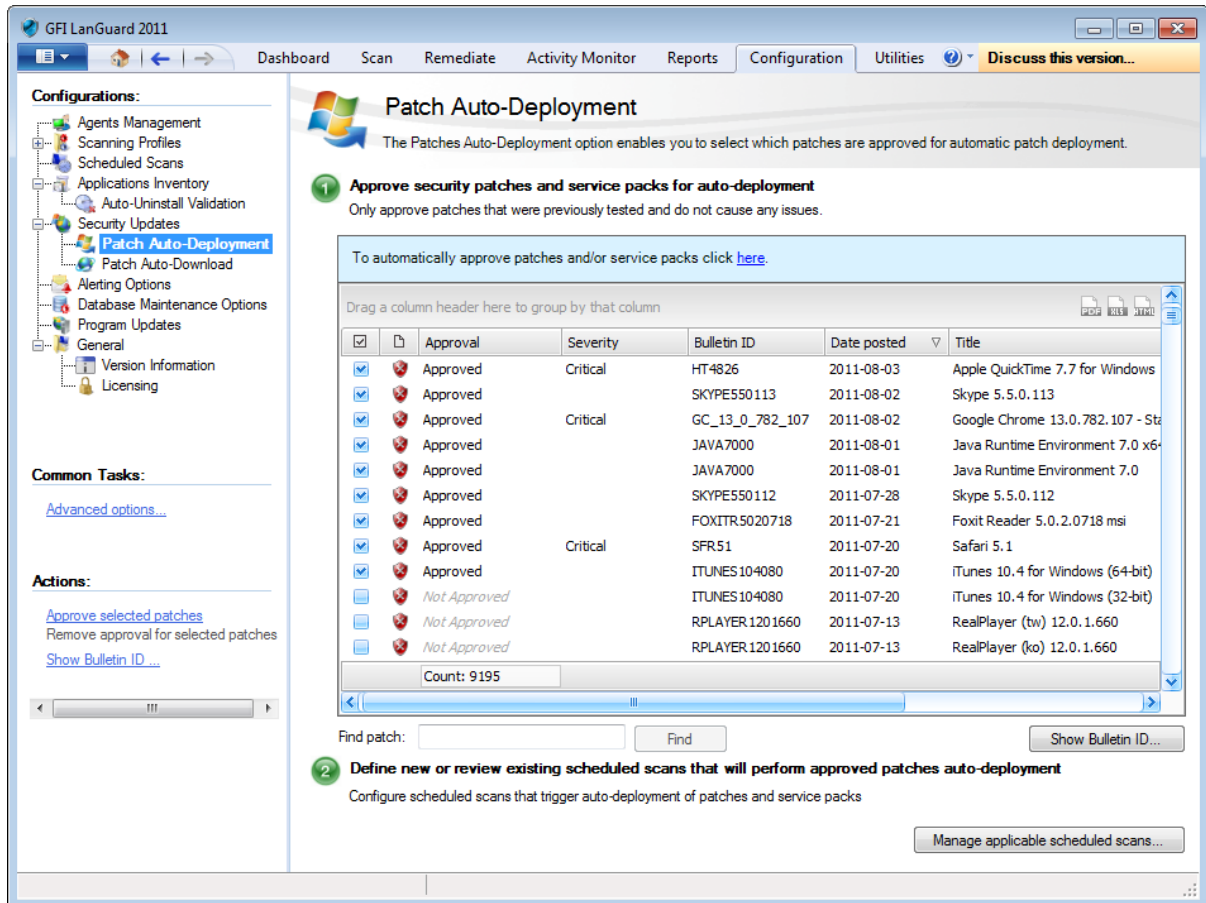
6.4.1 Patch Auto-deployment settings

GFI LanGuard ships with a patch auto-deployment feature, that enables you to automatically deploy missing patches and service packs in all 38 languages supported by Microsoft products. GFI LanGuard also supports patching of third party (Non-Microsoft) patches. For a complete list of supported third party applications visit:

<http://www.gfi.com/lannetscan/3pfullreport.htm> .

To configure patch auto-deployment:

1. Click on the **Configuration** tab ► **Security updates** ► **Patch Auto-Deployment**.
2. In the right pane, select the patches to auto-deploy.

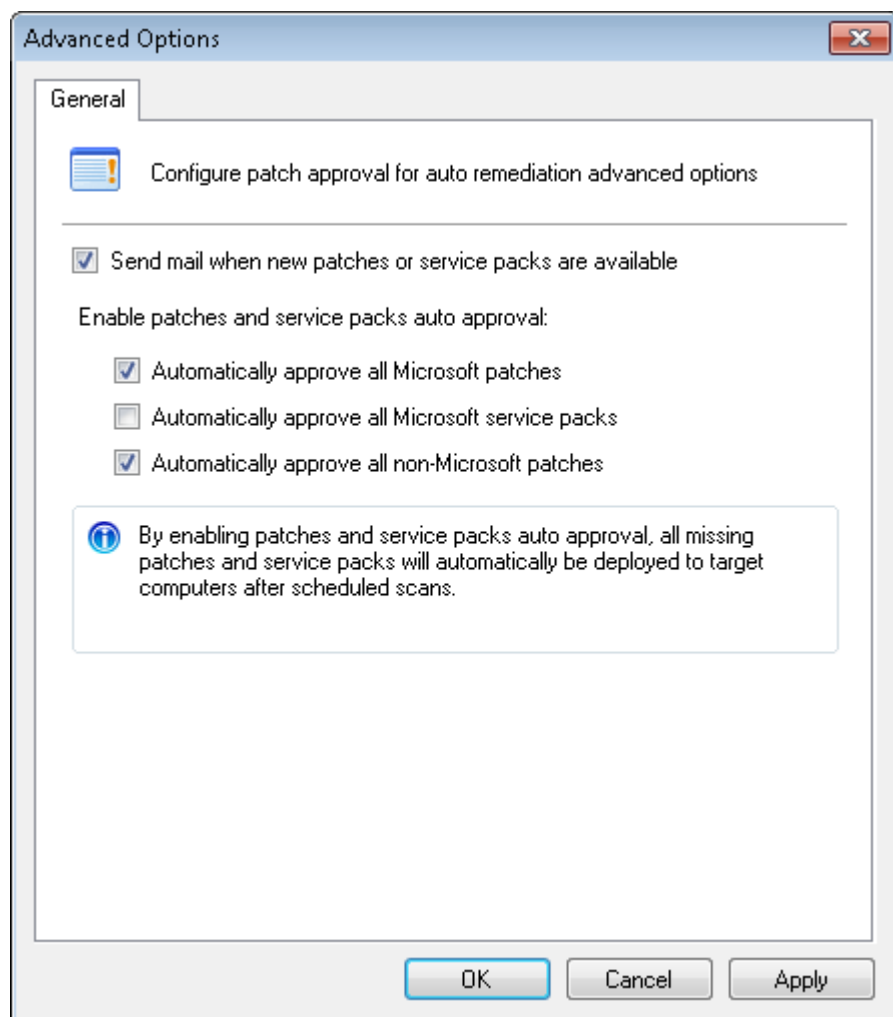


Screenshot 87 - Patch auto-deployment

Advanced Options

To configure auto-remediation:

1. Click **Configuration** tab ► **Security Updates** ► **Patch Auto-Deployment** and from **Common Tasks**, click **Advanced options**.



Screenshot 88 - Patch Auto-Deployment Advanced Options

2. Select the appropriate check boxes and click **OK** to save changes.

Manage applicable scheduled scans

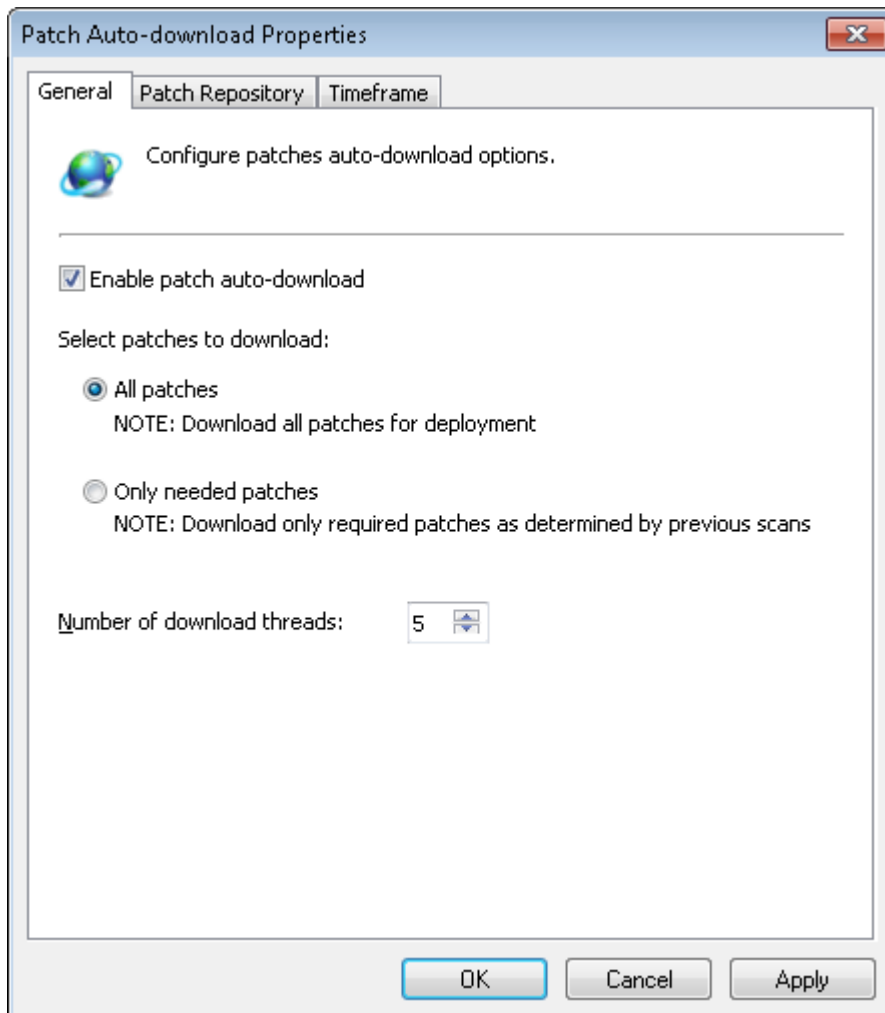
The **Manage applicable scheduled scan...** option enables you to configure scheduled scans that trigger auto-deployment of patches and service packs. For more information on how to use the **Manage applicable scheduled scan** feature refer to [Managing scheduled scans](#) section in this manual.

6.4.2 Patch Auto download settings

GFI LanGuard ships with a patch auto-download feature, that enables the automatic download of missing patches and service packs in all 38 languages supported by Microsoft products. In addition, you can also schedule patch auto-download by specifying the timeframe within which the download of patches is performed.

To configure patch auto-download:

1. Click **Configuration** tab ► **Security updates** ► **Patch Auto-Download**.
2. From the right pane, click the link.



Screenshot 89- Configuring Patch Auto-download Properties

3. In the General tab, select between **All patches** or **Only needed patches**.



Selecting **All patches**, downloads all patches issued by Microsoft, regardless of whether these are required for deployment. The **Only needed patches** option downloads only patches required for deployment.

4. To change the location where the downloaded patches are stored click the **Patch Repository** tab and specify the required details.
5. To change the timeframe during which patch downloads are performed, click on the **Timeframe** tab and specify the required details.



GFI LanGuard can use patch files downloaded by Microsoft WSUS when deploying missing patches and service packs on target computers. To use Microsoft WSUS downloaded files, select **Use files downloaded by Microsoft WSUS when available** and specify the Microsoft WSUS downloaded patches location.

6. Click **OK** to finalize settings.

6.5 Configuring alerting options

To configure alerting options:

1. Click **Configuration** tab ► **Alerting options**.
2. Click the link in the right pane.

Alerting Options Properties

General | **Daily digest**

Specify SMTP server and email address details for email notifications after each scheduled scan.

To: administrator@mydomain.com

CC: manager@mydomain.com

From: languard@mydomain.com

Server: localhost

Port: 25

☒ SMTP Server requires login

User name: administrator

Password: ●●●●●●●●●●

Verify Settings

OK **Cancel** **Apply**

Screenshot 90 - Configuring Alerting Options

3. Key-in the parameters described in Table 38 below:

Table 38 - Mail settings parameters

OPTION	DESCRIPTION
To	The recipient email address. Emails send by GFI LanGuard are received by this email address.
CC	Key-in another email address in this field if you need to send a copy to another email address.
From	The sender email address. GFI LanGuard will use this email account to send the required emails.
Server	Defines the server through which emails are routed. This can be either an FQDN (Fully Qualified Domain Name) or an IP Address.
Port	Defines the IP port through which emails are routed. Default value is 25
SMTP Server requires login	Select this option if the SMTP server requires a username and password to authenticate.

4. Click on the **Verify Settings** button to verify email settings.
5. Click **OK** to finalize settings.

6.6 Database maintenance options

GFI LanGuard ships with a set of database maintenance options through which you can maintain your scan results database backend in good shape.

For example, you can improve product performance and prevent your scan results database backend from getting excessively large by automatically deleting scan results that are older than a specific number of months.

If you are using a Microsoft Access database backend, you can also schedule database compaction. Compaction enables you to repair any corrupted data and to delete database records marked for deletion in your database backend; ensuring the integrity of your scan results database.

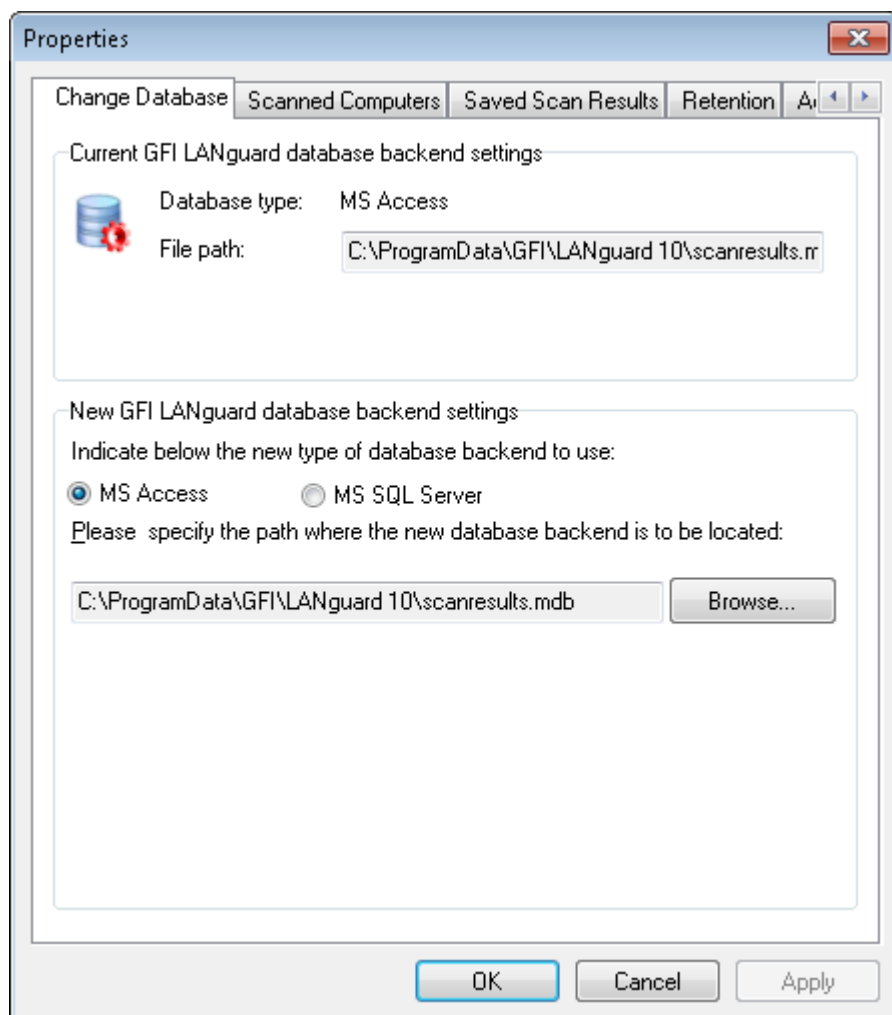
6.6.1 Selecting a database backend

GFI LanGuard supports both Microsoft Access and Microsoft SQL Server (2000 or higher) based database backend.

Storing scan results in a MS Access database backend

To store scan results in a Microsoft Access database:

1. Click **Configuration tab ► Database Maintenance Options ► Database backend settings...**



Screenshot 91 - The database maintenance properties dialog

2. Select the **MS Access** option and specify the full path (including the file name) of your Microsoft Access database backend.



The specified database file is created if it does not exist.



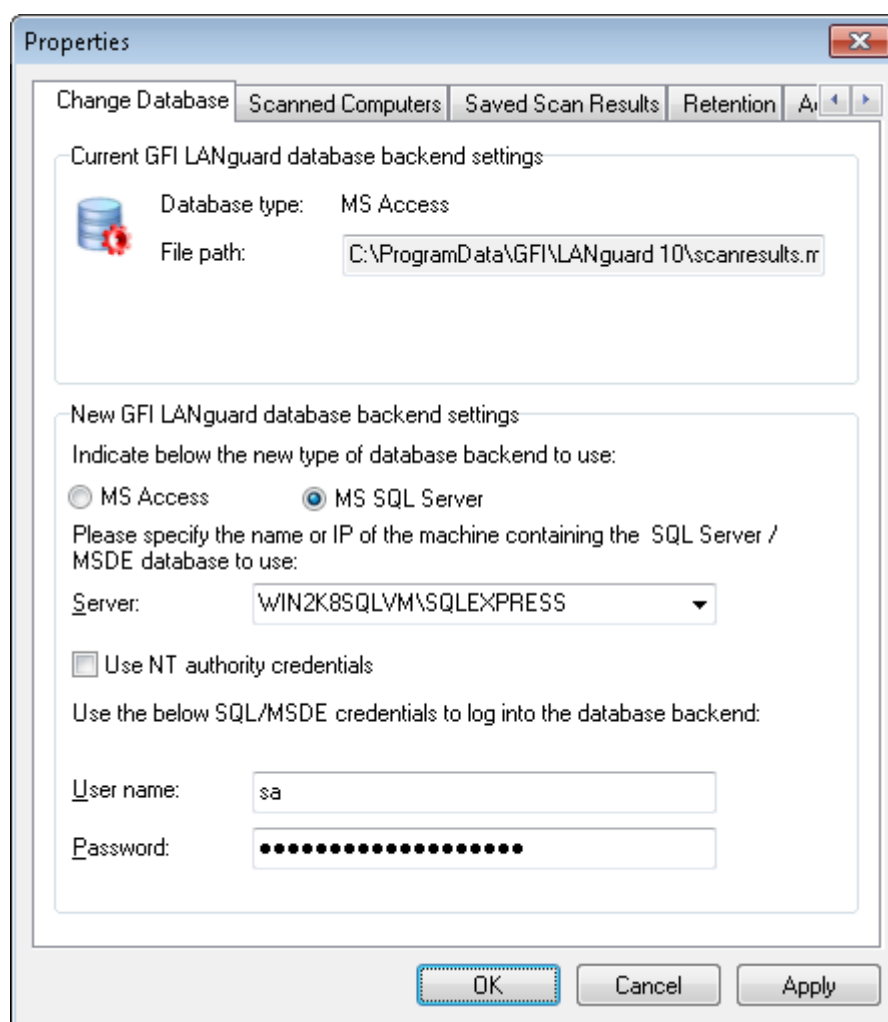
If the specified database file already exists and belongs to a previous version of GFI LanGuard, you are asked to over-write the existing information.

3. Click **OK** to finalize settings.

Storing scan results in an MS SQL Server database

To store scan results in a Microsoft SQL Server database:

1. Click **Configuration** tab ► **Database Maintenance Options** ► **Database backend settings...**



Screenshot 92 - Microsoft SQL Server database backend options

2. Select the **MS SQL Server** option and choose the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

3. Specify the SQL Server credentials or select the **Use NT authority credentials** option to authenticate to the SQL server using windows account details.

4. Click **OK** to finalize your settings.



If the specified server and credentials are correct, GFI LanGuard will automatically log on to your SQL Server and create the necessary database tables. If the database tables already exist, it will re-use them.

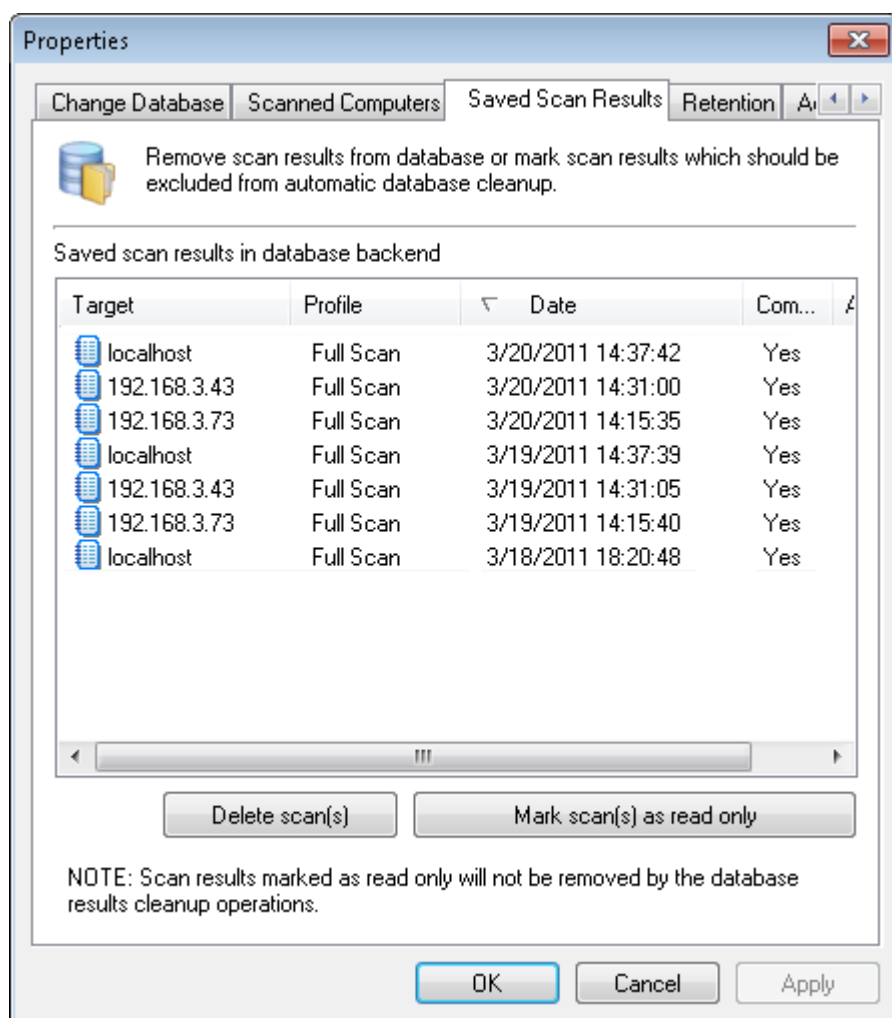


When using NT authority credentials, make sure that GFI LanGuard services are running under an account that has both access and administrative privileges on the SQL Server databases.

6.6.2 Managing saved scan results

Use the **Saved Scan Results** tab to maintain your database backend and delete saved scan results that are no longer required. Deletion of non-required saved scan results can be achieved manually as well as automatically through scheduled database maintenance.

During scheduled database maintenance, GFI LanGuard automatically deletes saved scan results that are older than a specific number of days/weeks or months. You can also configure automated database maintenance to retain only a specific number of recent scan results for every scan target and scan profile.



Screenshot 93 - Database maintenance properties: Managed saved scan results tab

To manage saved scan results:

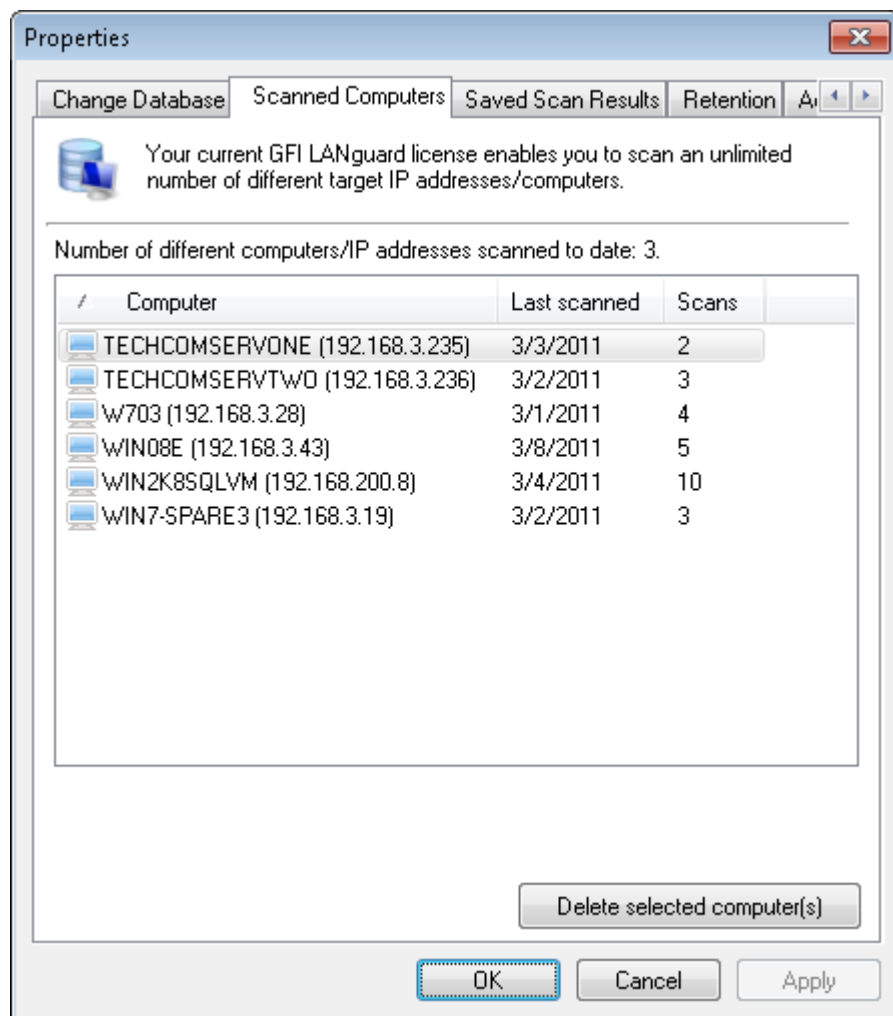
1. Click on the **Configuration** tab ► **Database Maintenance Options** ► **Manage saved scan results...**
2. To delete saved scan results, select the particular result(s) and click **Delete Scan(s)**.
3. To let GFI LanGuard manage database maintenance for you, select **Scans generated during the last** to delete scan results, which are older than a specific number of

days/weeks, or months or **Scans per scan target per profile in number of** to retain only a specific number of recent scan results.

6.6.3 Database maintenance: List of scanned computers

GFI LanGuard maintains a global list of scanned computers for licensing purposes. Any computers in excess of what is specified in the licensing information are not scanned.

GFI LanGuard enables systems administrators to delete scanned computers in order to release licenses that were previously utilized.



Screenshot 94 - Database maintenance properties: Scanned Computers tab

To delete computers previously scanned:

1. Click **Configuration tab ► Database Maintenance Options ► Manage list of scanned computers...**
2. Select the computers to delete and click **Delete selected computer(s)**.

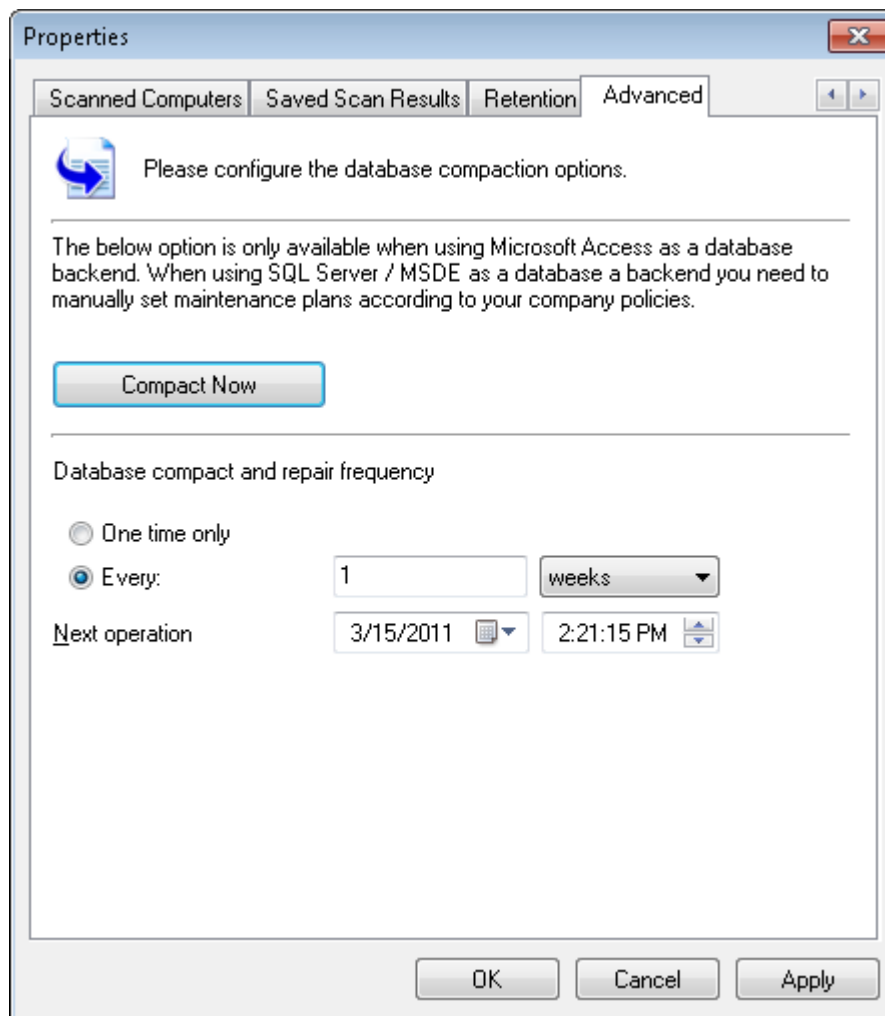


Deleting computers from the database is a one-way operation that will also delete all computer related data from the database. Once deleted, this data is no longer available.

6.6.4 Database maintenance: Advanced options

GFI LanGuard enables you to repair and compact the Microsoft Access database backend automatically to improve performance.

During compaction, the database files are reorganized and records that have been marked for deletion are removed. In this way, you can regain used storage space. During this process, GFI LanGuard also repairs corrupted database backend files. Corruption may occur for various reasons. In most cases, a Microsoft Access database is corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, unresponsive operations forced reboots, and so on).



Screenshot 95 - Database Maintenance properties: Advanced tab

To compact and repair a Microsoft Access database backend:

1. Click **Configuration** tab ► **Database Maintenance Options** ► **Database maintenance plan...**
2. To manually launch a repair and compact process on a Microsoft Access database backend, click **Compact Now**.
3. To automate the repair and compact process on an Microsoft Access database backend select **One time only** to schedule a onetime Microsoft Access database repair and compact or **Every** to execute a repair and compact process on a regular schedule. Specify the date, time and frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

6.6.5 Database maintenance: Retention options

Database retention options enable you to keep your database clean and consistent, by configuring GFI LanGuard to automatically delete unwanted scan results and scan history information while retaining important ones.

To configure retention settings:

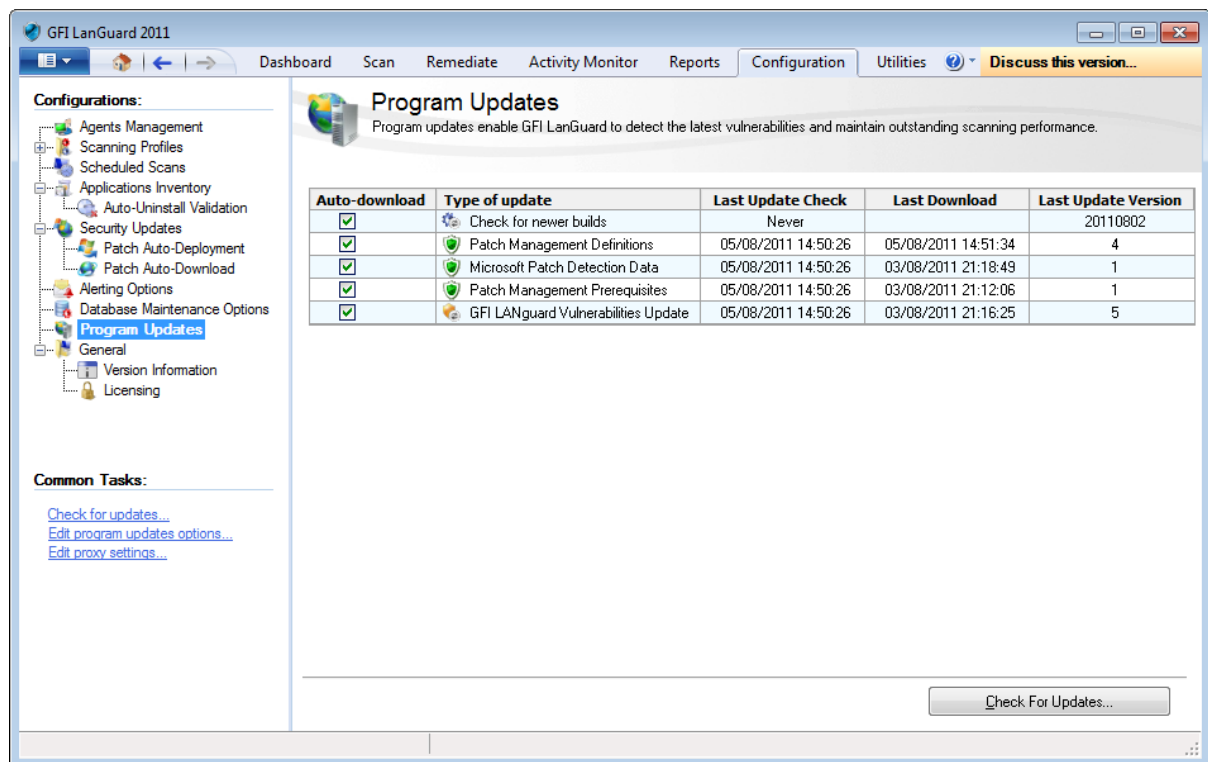
1. Click **Configuration** tab ► **Database Maintenance Options** ► **Database backend settings...** ► **Retention** tab.
2. Configure the options described in Table 39 below:

Table 39 - Database retention options

OPTION	DESCRIPTION
Keep scans generated during the last	Keep scan results generated during the specified number of days/weeks/months.
Keep scans per scan target per profile number of	Specify the number of scan results to keep, for every scan target by every scan profile.
Never delete history	Select this option if you want to keep all scan history.
Keep history for the last	Keep scan history for the specified number of days/weeks/months.

3. Click **OK** to finalize settings.

6.7 Program updates



Screenshot 96 - Program updates

This tool enables GFI LanGuard to detect the latest vulnerabilities and maintain its scanning performance. Configure GFI LanGuard to auto-download updates released by GFI to improve functionalities in GFI LanGuard. These updates also include checking GFI web site for newer builds. Updates can be enabled/disabled by selecting the checkbox in the **Auto-download** column.

GFI LanGuard can download all Unicode languages. This includes (but is not limited to) English, German, French, Italian, Spanish, Arabic, Danish, Czech, Finnish, Hebrew, Hungarian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Portuguese/Brazilian, Russian, Swedish, Chinese, Chinese (Taiwan), Greek, and Turkish.

6.7.1 Configure GFI LanGuard Proxy settings

To manually configure proxy server settings for internet updates:

1. Click on **Configuration** tab ► **Program Updates**.
2. From **Common Tasks** select **Edit proxy settings...**

GFI LanGuard Proxy Settings

General

Use this option to manually provide your proxy server settings.

☒ **Override automatic proxy detection**

☐ Connect directly to the Internet

☒ Connect via a proxy server

Server: 192.168.11.11:8080

☒ Proxy server requires authentication:

User name: administrator

Password: *****

Note: Patch file download, scheduled updates and some operations performed during the scanning process need to open Internet connections.

OK Cancel Apply

Screenshot 97 - Configuring proxy server settings

3. Select **Override automatic proxy detection**; configure the options described below:

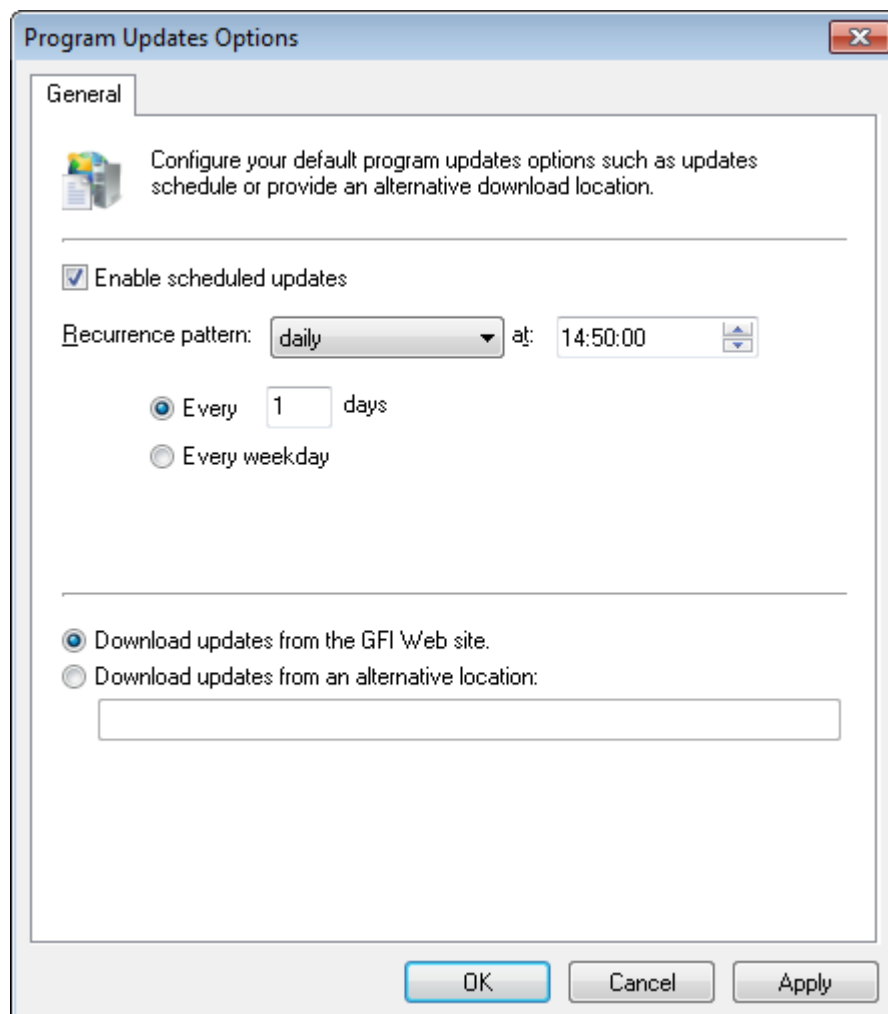
Table 40 - Proxy settings

OPTION	DESCRIPTION
Connect directly to the Internet	A direct internet connection is available.
Connect via a proxy server	Internet access is through a proxy server. Update the Server name and port number using this format <server>:<port>
Proxy server requires authentication	(Optional) Enter username and password if required by the proxy server.

6.7.2 Configure GFI LanGuard auto-updates options

GFI LanGuard can check for the availability of software updates at every program startup. To disable/enable this feature

1. Click on **Configuration** tab ► **Program Updates**. From **Common Tasks** select **Edit program updates options...**



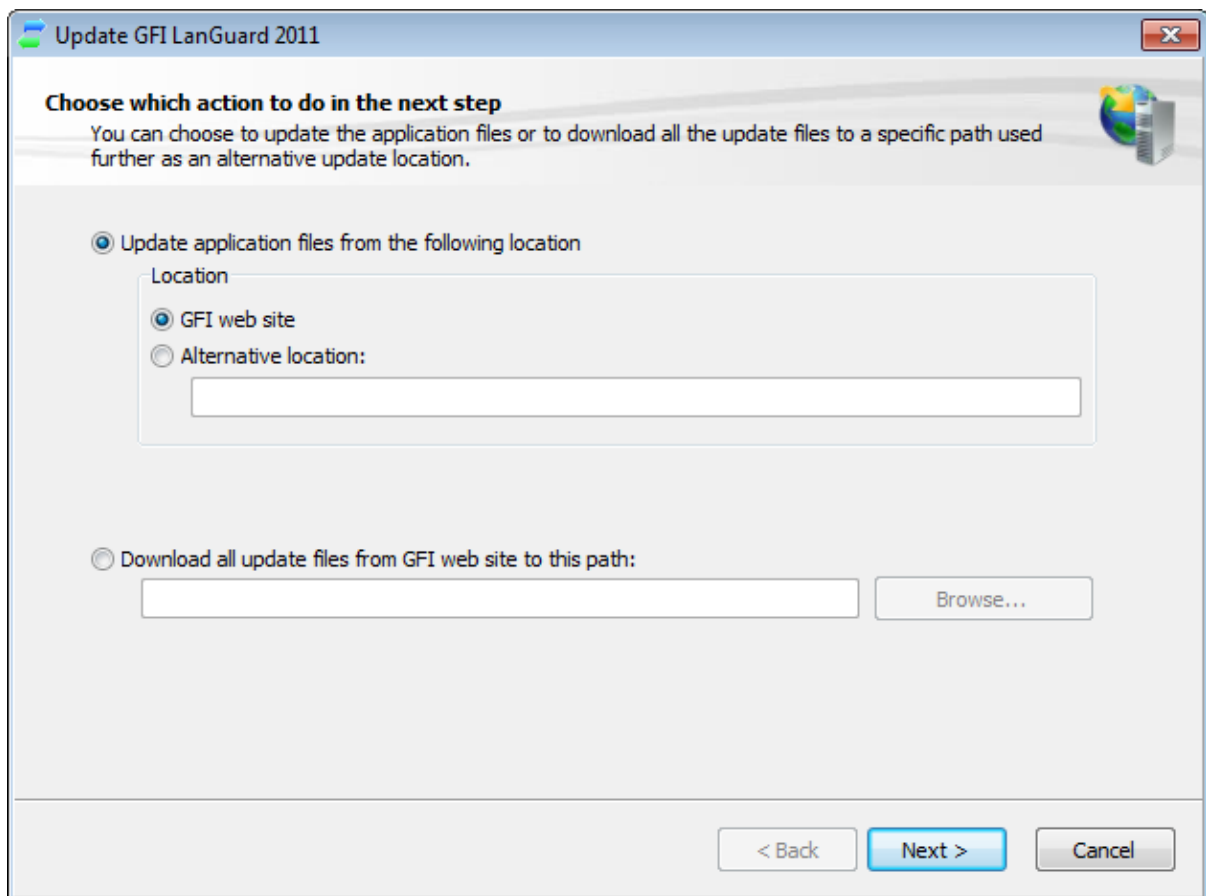
Screenshot 98 - Configure updates at application startup

2. Select/unselect **Check for updates at application startup** to enable/disable auto update checks at application startup.
3. Select/unselect enable scheduled updates to configure the frequency of update checks.
4. Specify whether GFI LanGuard download updates from GFI website or from an alternative location.
5. Click **OK** to finalize settings.

6.7.3 Starting program updates manually

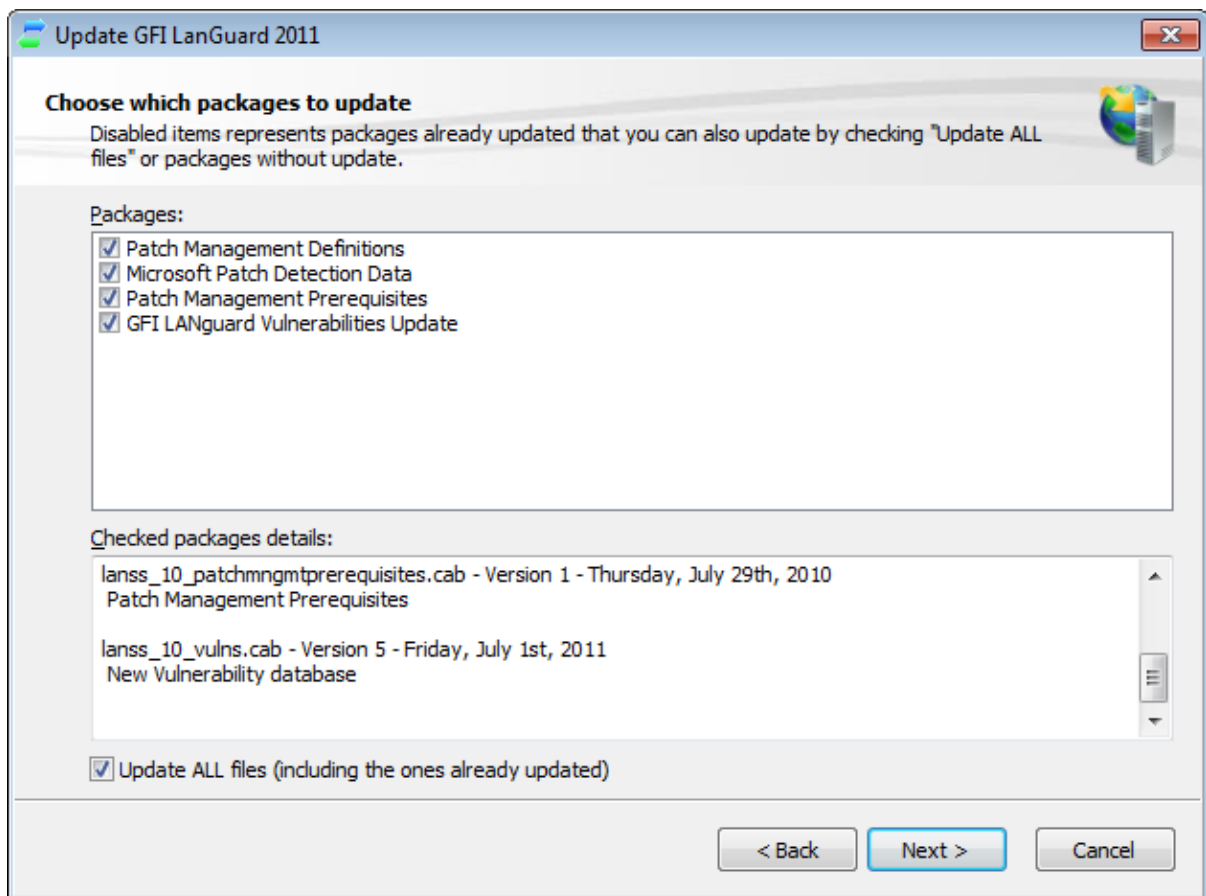
To start GFI LanGuard program updates manually:

1. Click on **Configuration** tab ► **Program Updates**.
2. From **Common Tasks** click **Check for updates**.



Screenshot 99 - The Check for Updates wizard: Stage 1

2. Specify the location from where the required update files will be downloaded.
3. (Optional) Change the default download path, select **Download all update files... to this path** to provide an alternate download path to store all GFI LanGuard updates.
4. Click **Next** to proceed with the update.



Screenshot 100 - The Check for updates Wizard

5. Select the updates and click **Next**.
6. Click **Start** to start the update process.

6.7.4 Product Updates Activity

GFI LanGuard maintains a comprehensive log of all updates activity. This information can be reviewed by clicking **Activity Monitor** tab ► **Product Updates Activity** node. This enables you to keep track of which updates are successfully or not.

6.8 Importing and Exporting Settings

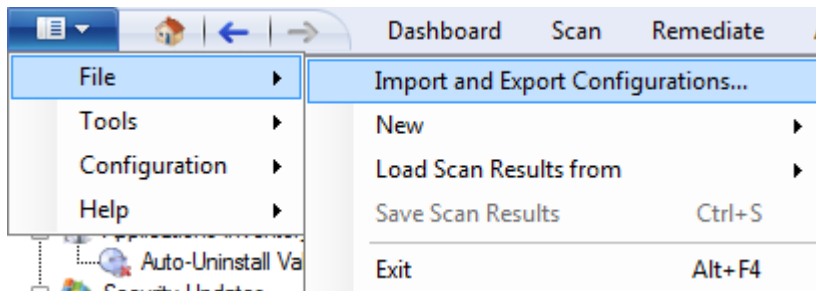
GFI LanGuard allows configurations, import and export, through **Import and Export Configurations...** in the **File** menu. Configurations that can be Imported/Exported include:

- » Scanning Profiles
- » Vulnerability Assessment
- » Ports (TCP/UDP)
- » Results Filtering Reports
- » Auto-Remediate Settings (Auto-Uninstall and Patch settings)
- » Options (Database Backend, Alerting, Schedule scan and Internal Settings)

6.8.1 Exporting Configurations from file

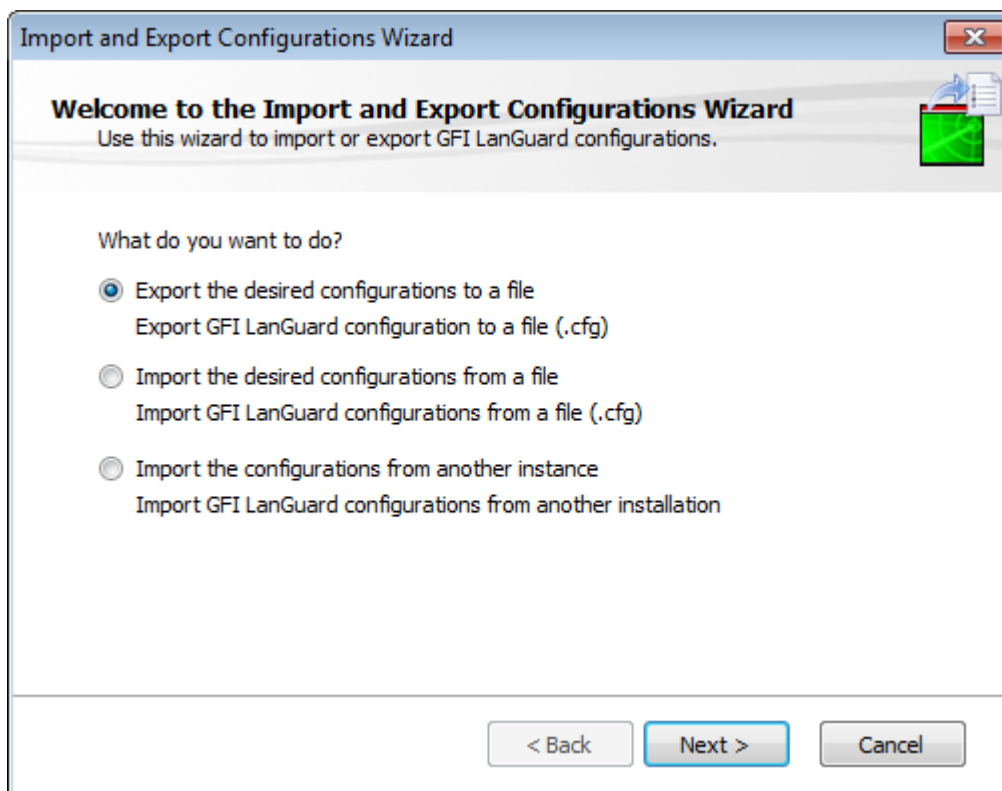
To export the configurations:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click the **GFI LanGuard** button ► **File ► Import and Export Configurations...**



Screenshot 101 - Import and Export Configuration

3. Select **Export** the desired configuration to a file and click **Next**.
4. Specify the path where to save the exported configuration, and click **Next**.



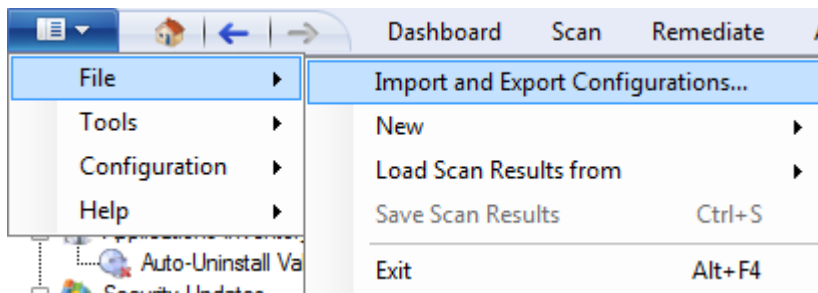
Screenshot 102 - Export configurations to file

5. Wait for the configuration tree to load and select the configurations to export. Click **Next** to start export.
6. A notify dialog will confirm that exporting is completed.
7. Click **OK** to finish.

6.8.2 Importing Configurations from file

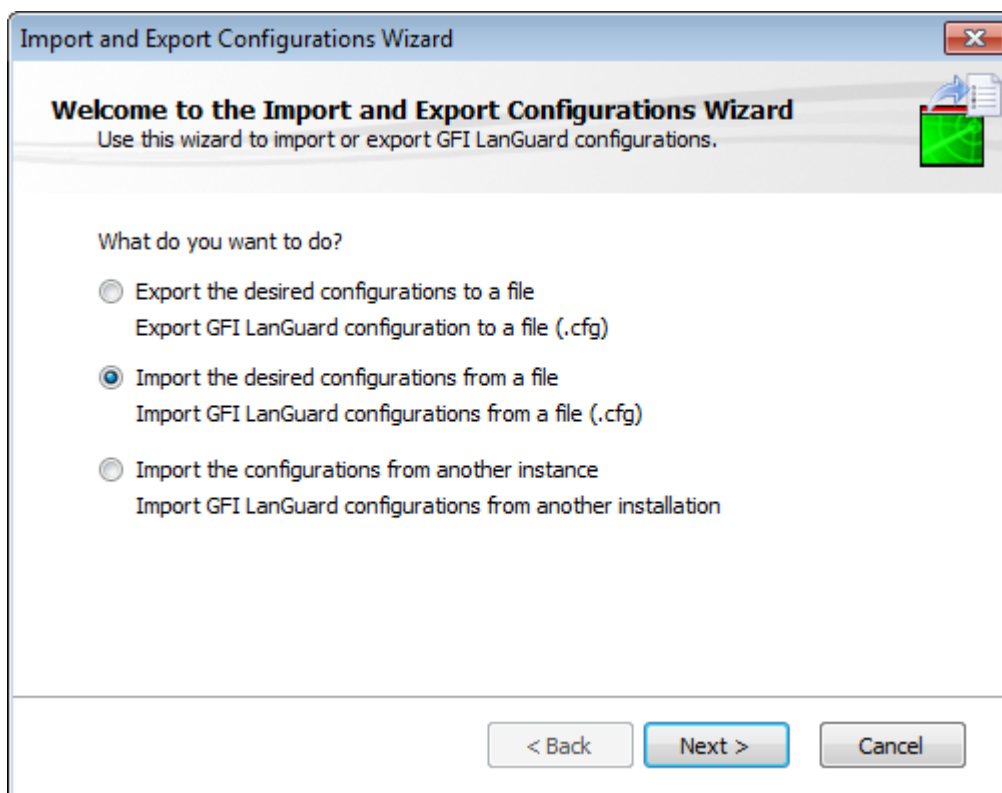
To import saved configurations:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.



Screenshot 103 - Import and Export Configurations

2. Click the **GFI LanGuard** button ► **File ► Import and Export Configurations...**
3. Select **Import** the desired configuration from a file and click **Next**.
4. Specify the path from where to load configuration, and click **Next**.
5. Wait for the configuration tree to load and select the configurations to import. Click **Next** to start import.

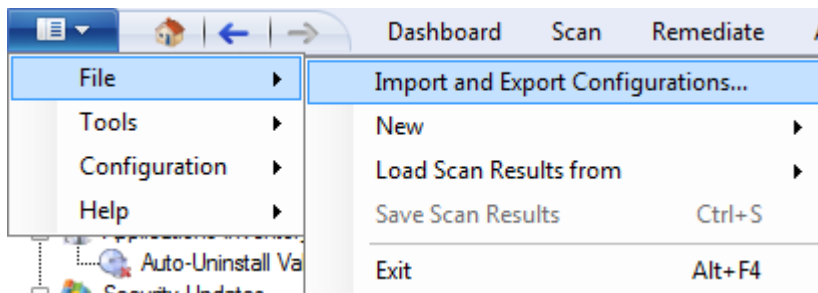


Screenshot 104 - Import configurations from a file

6. Confirm the override dialog box; by clicking, **Yes** or **No** as required.
7. A notify dialog will confirm that exporting is completed
8. Click **OK** to finish.

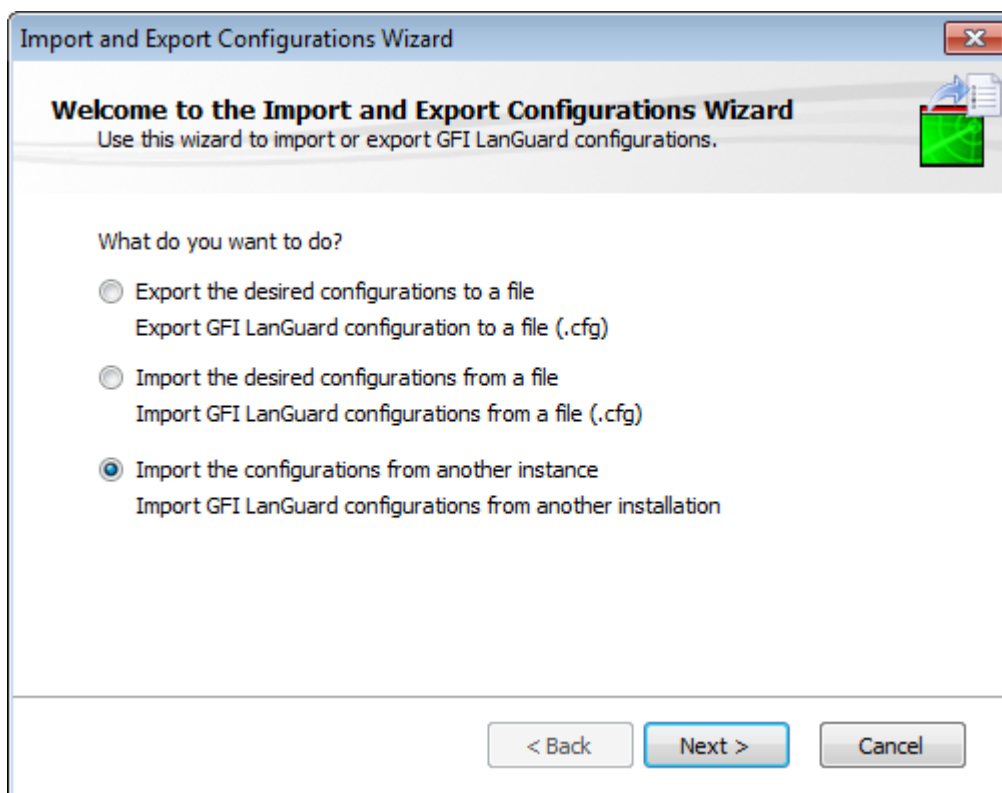
6.8.3 Import settings from another instance of GFI LanGuard

1. Launch the latest GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click the **GFI LanGuard** button ► **File ► Import and Export Configurations...** to launch the **Import and Export Configurations** wizard.



Screenshot 105 - Import and Export Configurations

3. Select **Import the configuration from another instance** and click **Next**.
4. Click **Browse** to select the GFI LanGuard installation folder. The default location is <Local Disk>\Program Files\GFI\ LanGuard <Version>. Click **Next**.



Screenshot 106 - Import setting

5. Select which settings you want to import and click **Next**.

6. While importing, GFI LanGuard will ask you whether you want to override or keep your settings. Select an option from Table 41 below:

Table 41 - Override options

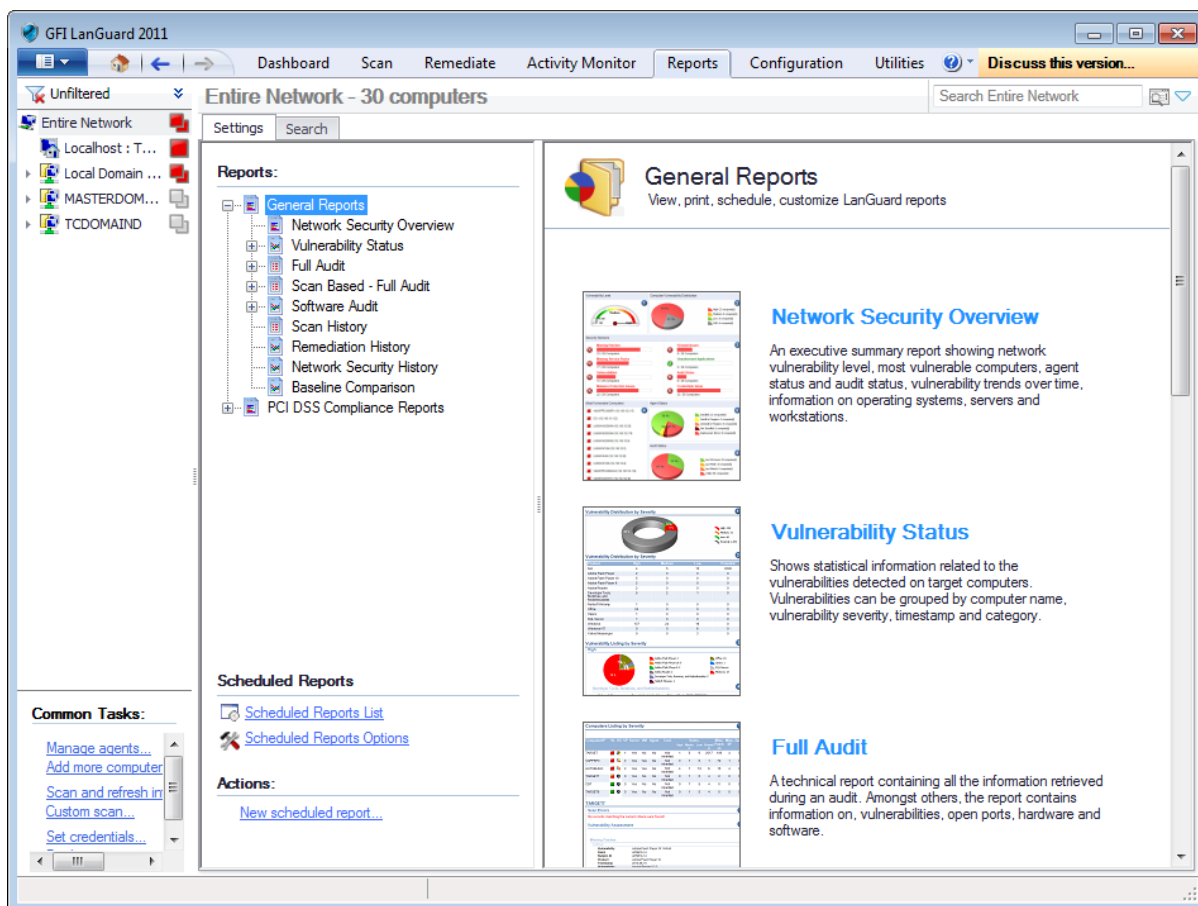
OPTION	DESCRIPTION
Yes	Override the current setting with the imported setting.
No	Keep the current setting and ignore the imported setting.
Auto Rename	Rename the imported settings and keep the current settings.

7. Click **OK** when the import is ready.

7 Reporting

7.1 Introduction

The **Reporting** tab enables you to generate technical IT level and management non-IT level reports based on network security audits carried out by GFI LanGuard. This chapter describes how to manage the reports in GFI LanGuard.



Screenshot 107 - Reporting tab

7.2 Available reports

Table 42 below describes the available reports in GFI LanGuard:

Table 42 - Available reports

REPORT NAME	DESCRIPTION
Network Security Overview	An executive summary report showing: » Network vulnerability level » Most vulnerable computers » Agent status » Audit status » Vulnerability trends over time » Information on operating systems » Servers and workstations.

REPORT NAME	DESCRIPTION
Computer Security Overview	An executive summary report showing: » Computer vulnerability level » Agent status » Audit status » Vulnerability trends over time » Computer summary and details.
Vulnerability Status	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by: » Computer name » Vulnerability severity » Timestamp » Category.
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.
Full Audit	A technical report showing information retrieved during an audit. Amongst others, the report contains information on: » Vulnerabilities » Open ports » Hardware and software.
Computer Summary	A summary of scan target information, including: » Operating system information » Agent status » Vulnerabilities severity.
Computers Detailed	Amongst other computer related details, this report includes information on: » The network role of a scan target » The domain name that the scan target is a member of » Registry » Shares » Users and groups.
Hardware Audit	Illustrates information related to the hardware found during an audit.
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.
Open Ports	Lists all the open ports found during an audit. The result are grouped by port type (TCP and UDP).
Scan Based - Full Audit	A technical report showing information retrieved during a specified scan. The report contains full details of the scanned computers and also auto-remediations performed after that scan.
Last Scan Summary	A technical report containing the summary of the information retrieved during the last scan.
Last Scan Details	A technical report containing all the information during the last scan. The report contains full details for the scanned target.
Last Auto-remediation	A technical report containing all the information related to auto-remediations performed after the last scan.
Last Scan Security Changes	Shows all changes detected during the last scan.
Software Audit	Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on: » Antivirus » Anti-spyware » Applications inventory.

REPORT NAME	DESCRIPTION
Unauthorized Applications	Lists all unauthorized applications installed scan targets.
Antivirus Applications	Shows information related to the antivirus installed on scan targets.
Scan History	An overview of the network security audits performed over time. Amongst others, the report includes information on: » Most scanned computers » Least scanned computers » Auditing status » History listing.
Remediation History	Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on: » Remediation actions per day » Remediation distribution by category » Remediation list grouped by computers.
Network Security History	Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to: » The vulnerability level » User accounts » Groups » Ports » Shares » Registry entries.
Baseline Comparison	Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on: » Registry » Installed service packs » Missing patches » Vulnerability level.

7.3 Generating reports

GFI LanGuard enables you to generate one-time reports or scheduled a reports. The sections below describe both scenarios.

7.3.1 One-time reporting

To generate a one-time reports:

1. Click **Reports** tab.
3. From the left pane, select if you want to report on the entire network or a specific scan target.
3. From **Reports**, select the report to generate.
4. Select items to report on.
5. (Optional) If you modified one of the default reports settings, GFI LanGuard enables you to save those settings as a new report. Click **Save as new report**.
6. Click **Generate report**.



Screenshot 108 - Report sample

7.3.2 Scheduled reports

GFI LanGuard enables you to automate reporting functions by scheduling reports. To schedule reports:

1. Click **Reports** tab.
2. From **Actions**, select **New scheduled report....**

GFI LanGuard Scheduled Reports
Manage GFI LanGuard Scheduled Reports

Add New Scheduled Report Add Schedule Cancel

1 Report Template

Schedule Report Template: Computer Security Overview

Schedule Report Name: Schedule for report 'Computer Security Overview'

Schedule Report Description: An executive summary report showing computer vulnerability level, agent status and audit status, vulnerability trends over time, computer details and summary.

2 Target Domains & Computers

Select target computers for the scheduled report

+ ×

TEMP

3 Scheduling Settings

☒ Enable schedule
Run the Report every day at 02:04.

☐ One time only, on: 05/08/2011 at: 02:04:34

☒ Recurrence pattern: daily at: 02:04:34

Daily recurrence pattern

☒ Every 1 days

☐ Every weekday

4 Alerting & Saving Settings

☐ Export to file
Click on the 'Export Settings' button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Export Settings

☒ Send by mail
Click on the 'Alerting Options' button to customize and configure the general alerting options.
Alerting Options

Add Schedule Cancel

Screenshot 109 - Scheduled reports settings

3. From **Schedule report template**, select the report template to generate.
4. (Optional) Key-in a valid report name and description.
5. Select your scan targets.
6. Configure the frequency of when the report is generated.
7. (Optional) Select **Export to file** and click **Export settings** to save the schedule report settings and use them with another report.

8. (Optional) Select **Send by email** and click **Alerting options** to send the report by email and configure alerting options.



For information about Alerting options, refer to [Configuring alerting options](#) section in this manual.

Scheduled reports options

To configure additional scheduled reports settings:

1. Click **Scheduled reports options**.
2. Click **Alerting Options** to configure email settings to use to send reports.
3. Click **Storage Options** to specify the format and the location where generated reports are saved.



By default, all generated reports are stored as **PDF** in:
C:\ProgramData\GFI\LanGuard 10\Reports.



For information about Alerting options, refer to [Configuring alerting options](#) section in this manual.

7.4 Custom reports

GFI LanGuard enables you to create new reports based on an existing report.

1. From the **Reports** tab, select the existing report.
2. From the report sample in the right panel, click **Customize report**.

Screenshot 110 - Customize the report parameters

3. Configure the parameters described in Table 43 below:

Table 43 - Customize report parameters

TAB NAME	DESCRIPTION
Report Items	Select the report items that will be included in the report. Check/Uncheck the report items.
Filters	Filter the report results. Select the criteria and key-in a value to be used as a filter.
Grouping & Sorting	Use this tab to configure sorting or grouping of report results. Select the group and the sorting order (Ascending or Descending).

4. Click **Save as new report...** and in the **Add report** dialog key-in a valid report name and an optional description.

5. Click **OK**.



The new report is created in the report node selected in step 1.

7.4.1 Customizing report logos

GFI LanGuard enables you to use your company / custom logo in the built-in reports included in the product. Any inserted logos are placed in the header or footer of the report depending on the name.

Customize report header logo

1. Create / select your image.
2. Resize image to: Width = 624, Height = 25.
3. Rename the image to **headerlogo.png**.
4. Copy / paste image in **Computer ► Local Disk (C:) ► ProgramData ► GFI ► LanGuard 10 ► Graphics ► Logo**.



For OS versions prior to Windows Vista, paste image in **My Computer ► C:\ ► Documents and Settings ► All Users ► Application Data ► GFI ► LanGuard 10 ► Graphics ► Logo**.

Customize report footer logo

1. Create / select your image.
2. Resize image to: Width = 109, Height = 41.
3. Rename the image to **footerlogo.png**.
4. Copy / paste image in **Computer ► Local Disk (C:) ► ProgramData ► GFI ► LanGuard 10 ► Graphics ► Logo**.



For OS versions prior to Windows Vista, paste image in **My Computer ► C:\ ► Documents and Settings ► All Users ► Application Data ► GFI ► LanGuard 10 ► Graphics ► Logo**.

7.4.2 Customize email report format

For each scheduled email report type, there is a predefined HTML format file that includes placeholders delimited with ‘%’ symbol (for example: %TITLE%, %NAME%). You can edit the HTML format, edit HTML style, move and delete placeholders to further customize the email body of generated reports. The default template location is:
C:\ProgramData\GFI\LanGuard 10\Templates\template_mailbody.xml.

Take into consideration that GFI LanGuard can only manage known placeholders (listed below) with their predefined role. Placeholders are usable in all scheduled report types. Table 44 below describes the customizable placeholders:

Table 44 - Report placeholders

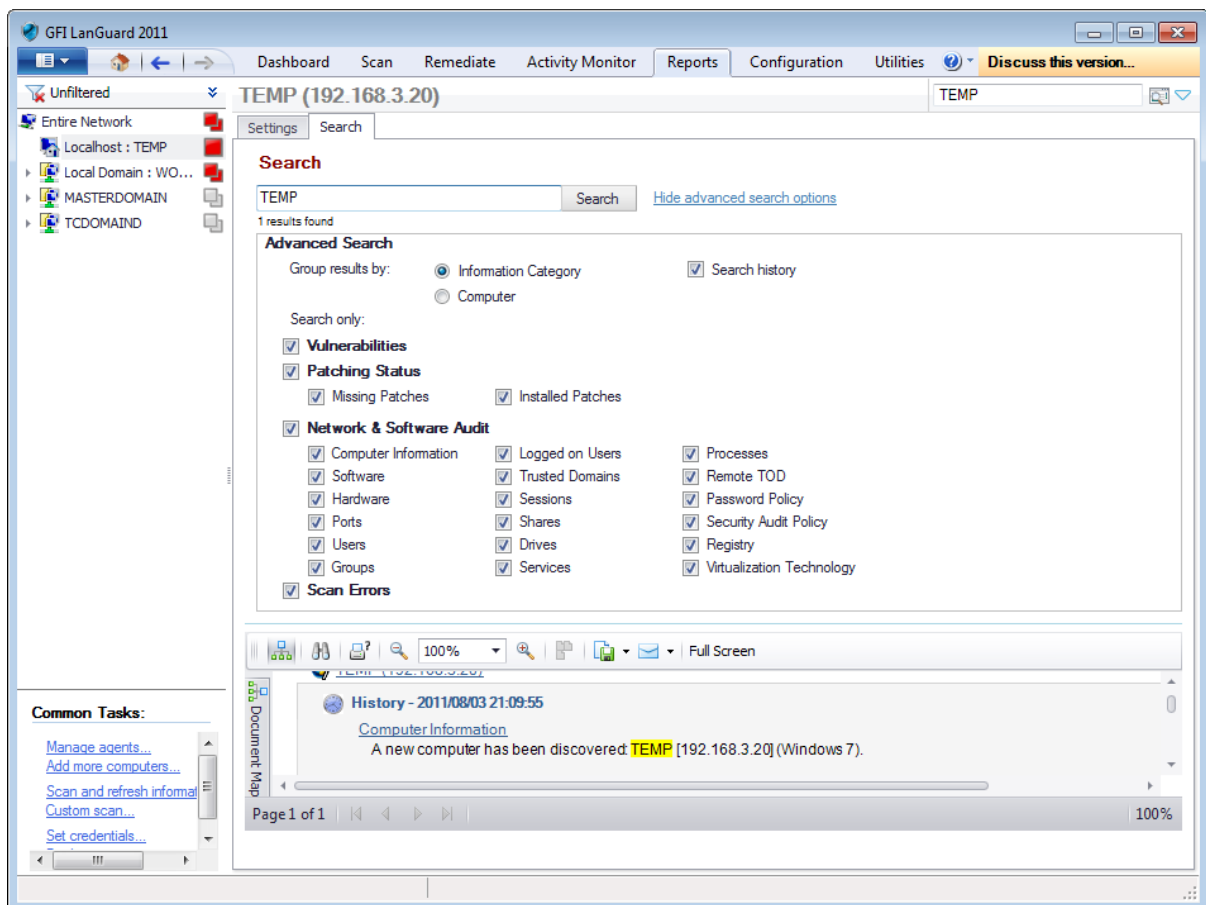
PLACEHOLDER	DESCRIPTION
%TITLE%	Email title for the generated report.
%NAME%	Scheduled report name.
%DESCRIPTION%:	Scheduled report description.
%TARGET%	Targets (computers, domains) represented in the scheduled report.
%LAST_RUN%	Last run date and time of the scheduled report.
%NEXT_RUN%	Next run date and time of the scheduled report. Note: this placeholder is used only for daily digest reports.
%PROFILE%	Scanning profile used whilst running the scheduled scan. Note: this placeholder is used only for post-scheduled scan reports.
%DURATION%	Scheduled scan duration. NOTE: this placeholder is used only for post-scheduled scan reports.
%ITEMS_COUNT%	Collected items count. NOTE: this placeholder is used only for post-scheduled scan reports.
%AUTOREMED_MISSINGPATCHES%	Used in the report if Auto-remediate Missing Patches option is enabled for the scheduled scan. NOTE: this placeholder is used only for post-scheduled scan reports.
%AUTOREMED_MISSINGSPS%	Used in the report if Auto-remediate Missing Service Packs option is enabled for the scheduled scan. NOTE: this placeholder is used only for post-scheduled scan reports.
%AUTOREMED_UNINSTAPPS%	Used in the report if Auto-remediate Uninstall Applications option is enabled for the scheduled scan. NOTE: this placeholder is used only in post-scheduled scan reports.

7.5 Full text searching

The full text search feature returns results in a structured and configurable manner. Any returned results offer clickable links for further details.

To use the full text search feature:

1. Click **Reports** tab and **Search** sub tab.
2. Enter you search item and click **Search**.



Screenshot 111 - Customize the report parameters

3. (Optional) Click **Advanced search** to configure filters to narrow your search results to something more specific.
4. Analyze the search results from the results section at the bottom.

8 Scanning Profiles

8.1 Introduction

GFI LanGuard enables you to scan your IT infrastructure for particular vulnerabilities using pre-configured sets of checks known as **scanning profiles**. Scanning profiles enable you to scan your network targets and enumerate only specific information. For example, you may want to use a scanning profile that is set to be used when scanning the computers in your DMZ as opposed to your internal network.

In practice, scanning profiles enable you to focus your vulnerability scanning efforts on to a specific area of your IT infrastructure such as identifying only missing security updates. The benefit is that you have less scan results data to analyze; tightening up the scope of your investigation and quickly locate the information that you require more easily.

Through multiple scanning profiles, you can perform various network security audits without having to go through a reconfiguration process for every type of security scan required.

8.2 Scanning profile description

Out of the box, GFI LanGuard includes an extensive list of scanning profiles as described below.

8.2.1 Complete/Combination scans

Table 45 below describes in detail the scans involved in the Complete/Combination scanning profile:

Table 45 - Complete/Combination scanning profiles

COMPLETE/COMBINATION SCANNING PROFILES	
Full Vulnerability Assessment	Use this scanning profile to enumerate particular network vulnerabilities such as open TCP/UDP ports commonly exploited by Trojans as well as missing patches and service packs. The list of vulnerabilities enumerated by this profile can be customized through the Vulnerabilities tab. Installed USB devices and applications are not enumerated by this profile. This profile will scan for all vulnerabilities. This includes vulnerabilities which have an associated Microsoft patch to them and which are considered missing patches.
Full Scan (Active)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN environments.
Full Scan (Slow Networks)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more... The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with WAN environments.

8.2.2 Vulnerability Assessment

Table 46 below describes in detail the scans involved in the Vulnerability Assessment scanning profile:

Table 46 - Vulnerability assessment scanning profiles

VULNERABILITY ASSESSMENT SCANNING PROFILES	
Top SANS 20 Vulnerabilities	Use this scanning profile to enumerate all vulnerabilities reported in the SANS top 20 list.
High Security Vulnerabilities	Use this scanning profile to enumerate open TCP/UDP ports and high security vulnerabilities. The list of TCP/UDP ports and high security vulnerabilities that will be enumerated by this profile can be customized through the TCP/UDP Ports tabs and the Vulnerabilities tab respectively.
Last Year's Vulnerabilities	Use this scanning profile to enumerate network vulnerabilities that emerged during the last 12 months.
Only Web	Use this scanning profile to identify web-server specific vulnerabilities. This includes scanning and enumerating open TCP ports that are most commonly used by web-servers such as port 80. Only TCP ports commonly used by web-servers are scanned by this profile. Network auditing operations as well as enumeration of vulnerabilities and missing patches are not performed using this profile.
Missing Patches	Use this scanning profile to enumerate missing patches. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.
Critical Patches	Use this scanning profile to enumerate only missing patches that are tagged as critical. The list of critical patches that will be enumerated by this profile can be customized through the Patches tab.
Last Month's Patches	Use this scanning profile to enumerate only missing patches that were released last month. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.
Only Service Packs	Use this scanning profile to enumerate missing service packs. The list of service packs that will be enumerated by this profile can be customized through the Patches tab.

8.2.3 Network & Software Audit

Table 47 below describes in detail the scans involved in the Network and Software audit scanning profile:

Table 47 - Network and Software audit scanning profiles

NETWORK AND SOFTWARE AUDIT SCANNING PROFILES	
Trojan Ports	Use this scanning profile to enumerate open TCP/UDP ports that are commonly exploited by known Trojans. The list of TCP/UDP ports to be scanned can be customized through the TCP Ports and UDP Ports tabs respectively. Only the TCP/UDP ports commonly exploited by known Trojans are scanned by this profile. Network auditing operations as well as enumeration of other open TCP/UDP ports and missing patches are not performed by this profile.
Port Scanner	Use this scanning profile to enumerate open TCP/UDP ports including those most commonly exploited by Trojans. The list of ports that will be enumerated by this profile can be customized through the TCP/UDP ports tab.
Software Audit	Use this scanning profile to enumerate all software applications installed on scan targets. This includes security software such as anti-virus and anti-spyware.
Full TCP & UDP Scan	Use this scanning profile to audit your network and enumerate all open TCP and UDP ports.
Only SNMP	Use this scanning profile to perform network discovery and retrieve information regarding hardware devices (routers, switches, printers, etc.) that have SNMP enabled. This enables you to monitor network-attached devices for conditions that require administrative attention.
Ping Them All	Use this scanning profile to audit your network and enumerate all computers that are currently connected and running.

NETWORK AND SOFTWARE AUDIT SCANNING PROFILES	
Share Finder	Use this scanning profile to audit your network and enumerate all open shares either hidden or visible. No vulnerability checks are performed by this profile.
Uptimes	Use this scanning profile to audit your network and identify how long each computer has been running since the last reboot.
Disks Space Usage	Use this scanning profile to audit your network and retrieve system information on available storage space.
System Information	Use this scanning profile to retrieve system information such as operating system details, wireless/virtual/physical network devices connected, USB devices connected, installed applications and more.
Hardware Audit	Use this scanning profile to audit your network and enumerate all hardware devices currently connected to your network computers.
Network Discovery	Use this scanning profile to enumerate any IP enabled device connected to your network.

8.2.4 Which scanning profile shall I use?

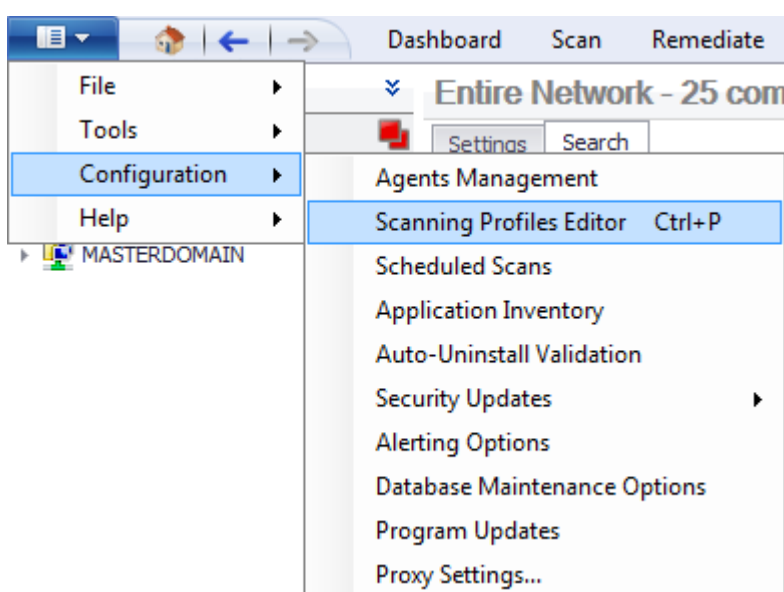
Select the scanning profile based on the:

- » **Scope of your vulnerability analysis, that is, what you want to achieve out of your vulnerability scan. Based on these factors, you can determine the type of vulnerability checks to be performed and the information that you want to retrieve from your scan targets.**
- » **Time you have at your disposal for target vulnerability scanning. The more vulnerability checks you run the longer it will take the scan process to complete.**

8.2.5 Creating a new scanning profile

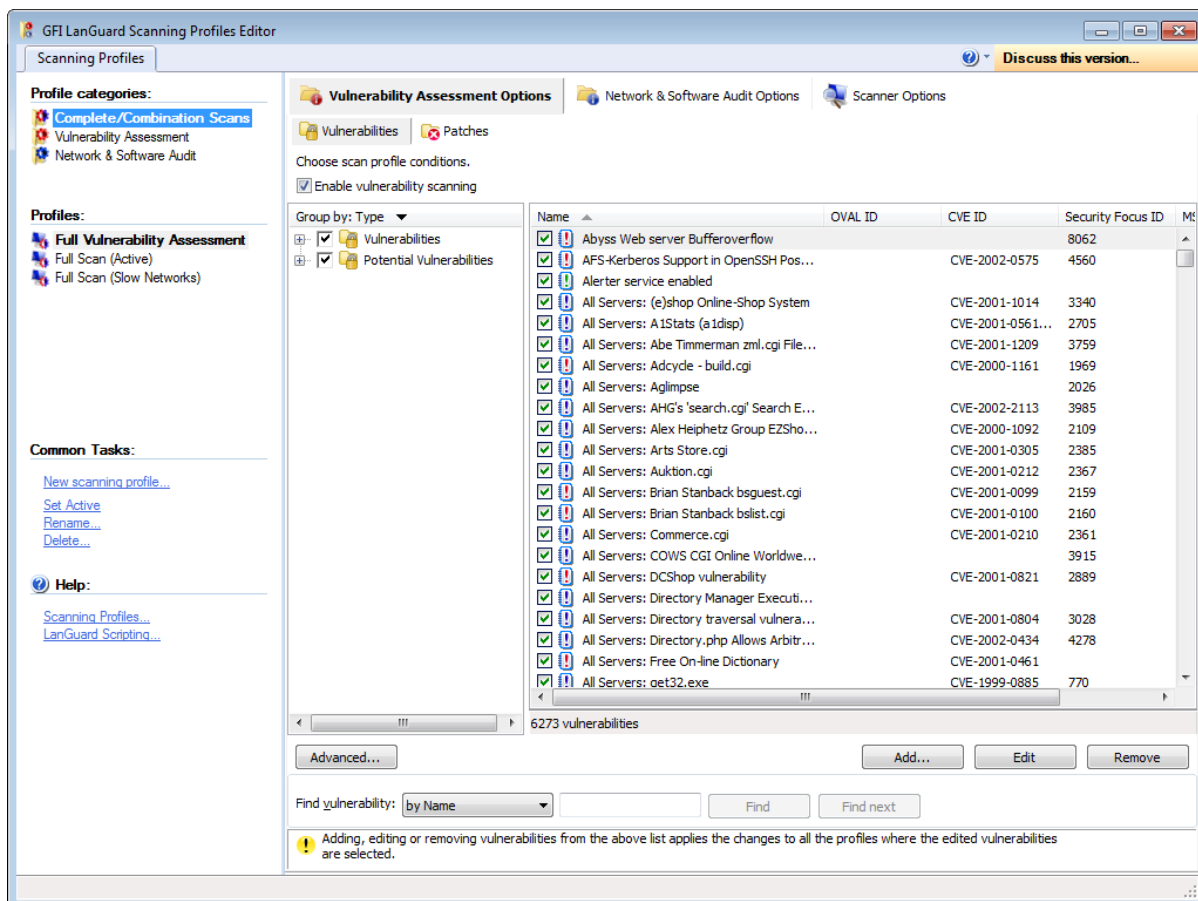
The **Scanning Profiles Editor** allows you to create new scanning profiles. To create a new custom scanning profile:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click the **GFI LanGuard button ► Configuration tab ► Scanning Profile Editor**.



Screenshot 112 - Launch the scanning profiles editor

3. In **Scanning Profiles Editor** from **Common Tasks**, click **New scanning profile...**

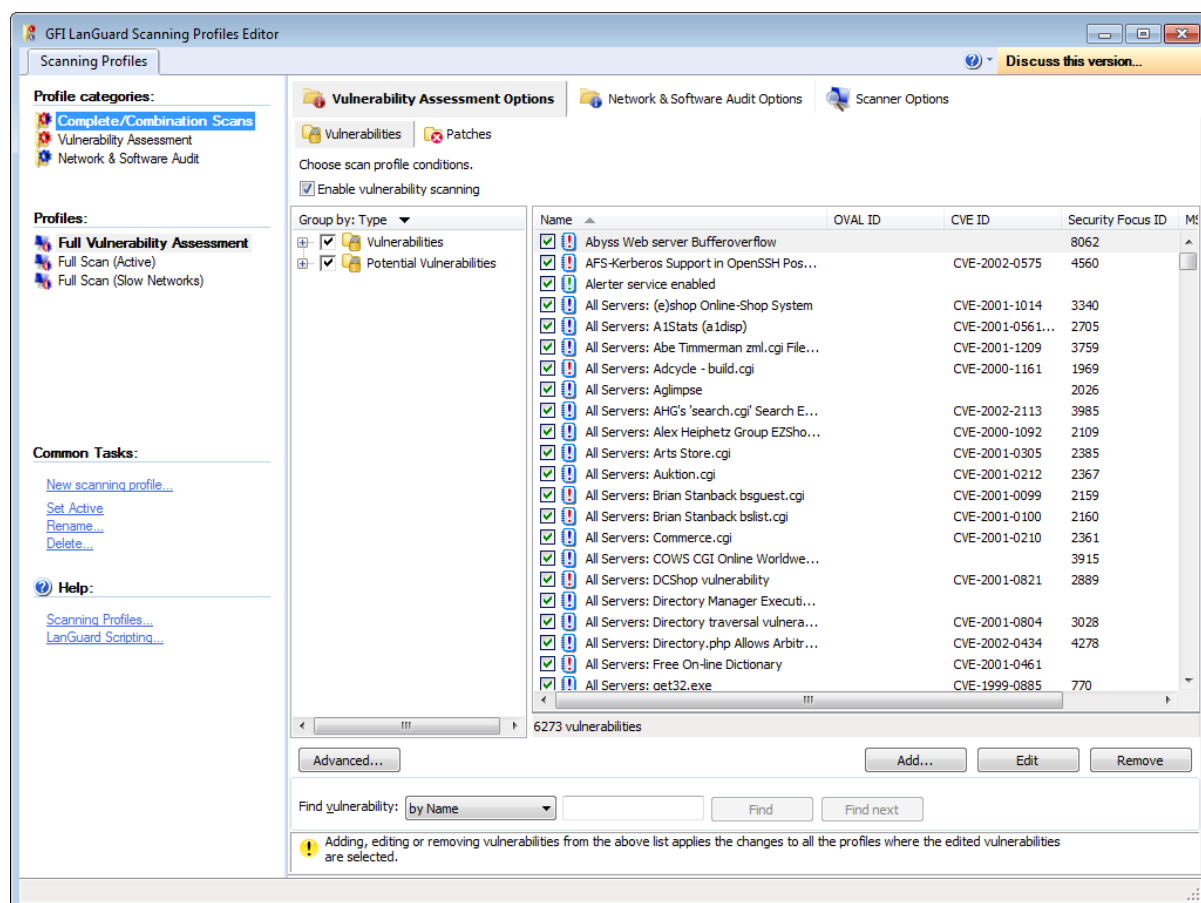


Screenshot 113 - The Scanning Profile Editor

4. Specify the name of the new profile and optionally select **Copy all settings from an existing profile** to clone settings from an existing profile.
5. Click **OK** to save settings. The new scanning profile is added under **Profiles** in the left pane.

8.3 Configure Vulnerabilities Assessment options

The scanning profiles that ship with GFI LanGuard are already pre-configured to run a number of vulnerability checks on selected target. You can however disable vulnerability scanning as well as customize the list of vulnerability checks executed during a scan.



Screenshot 114 - Scanning Profiles properties: Vulnerabilities tab options

8.3.1 Configure Vulnerabilities

To enable vulnerability scanning:

1. From the **Vulnerability Assessment Options** tab, click **Vulnerabilities** sub-tab.
2. Select the scanning profile to customize from the left pane under **Profiles**.
3. In the right pane, select **Enable Vulnerability Scanning** option.

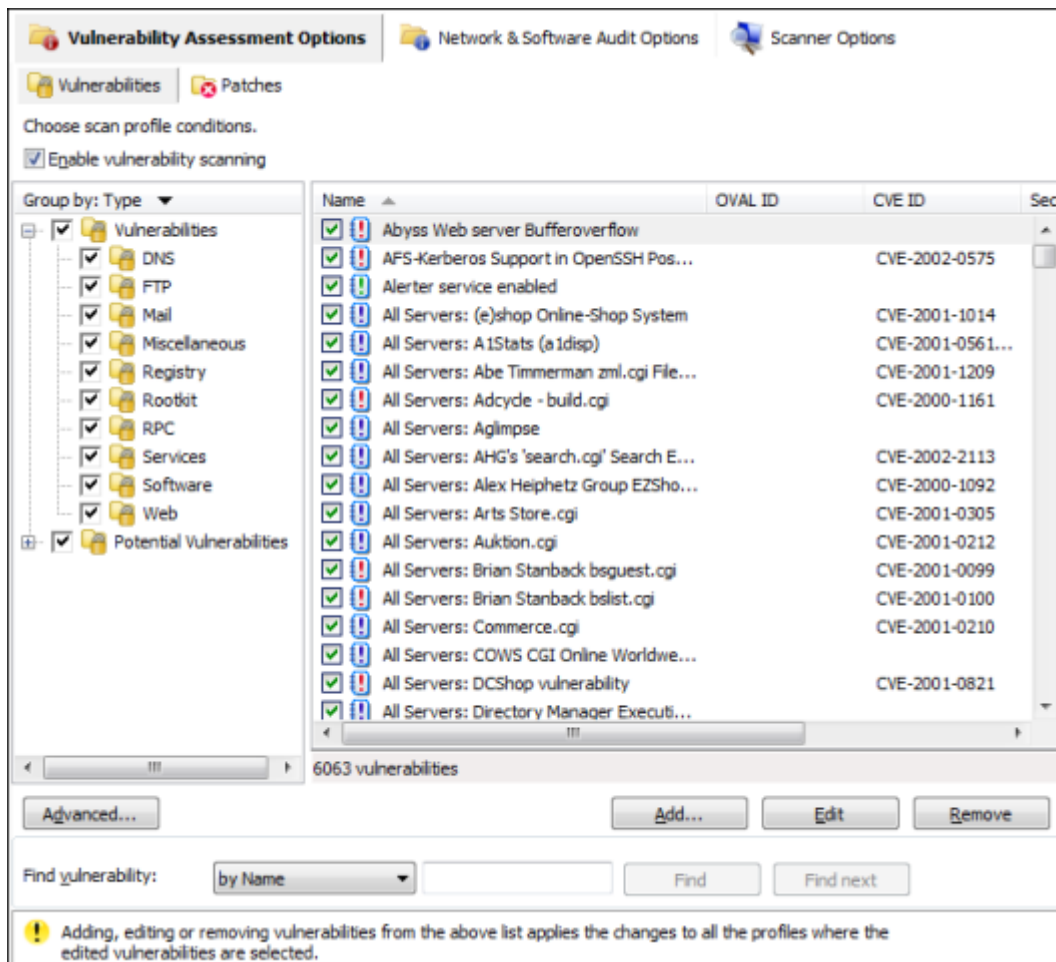


Vulnerability scanning is configured on a scan profile by scan profile basis. If in a particular profile this option is not selected, no vulnerability tests will be performed in the security audits carried out by this scanning profile.

Customizing the list of vulnerabilities to be scanned

To specify which vulnerabilities will be enumerated and processed by a scanning profile during a security audit:

1. From **Vulnerability Assessment Options** tab, select the scanning profile to customize from the left pane under **Profiles**.

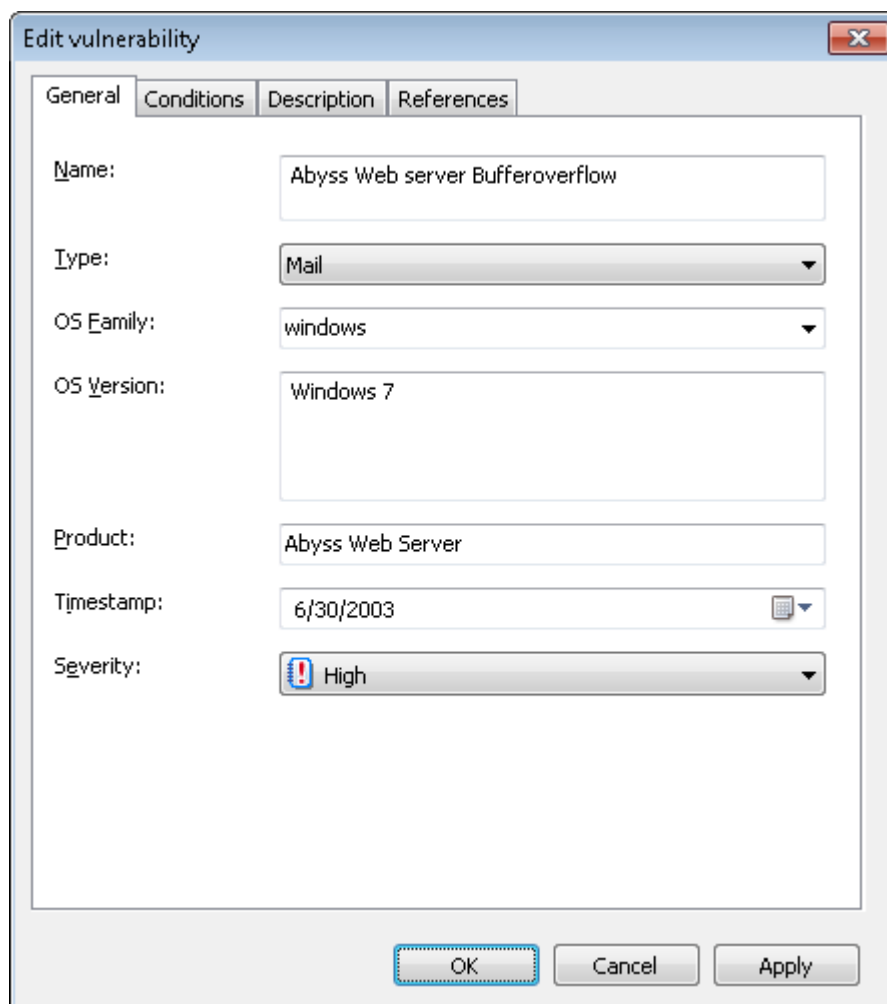


Screenshot 115 - Select the vulnerability checks to be run by this scanning profile

2. In the right pane, select the vulnerability checks to execute through this scanning profile.

Customizing the properties of vulnerability checks

All the checks listed in the **Vulnerabilities** tab have specific properties that determine when the check is triggered and what details will be enumerated during a scan.



Screenshot 116 - Vulnerability properties dialog: General tab

To change the properties of a vulnerability check:

1. Right-click on the vulnerability to customize, select **Properties**.
2. Customize the selected vulnerability check from the tabs described in Table 48 below:

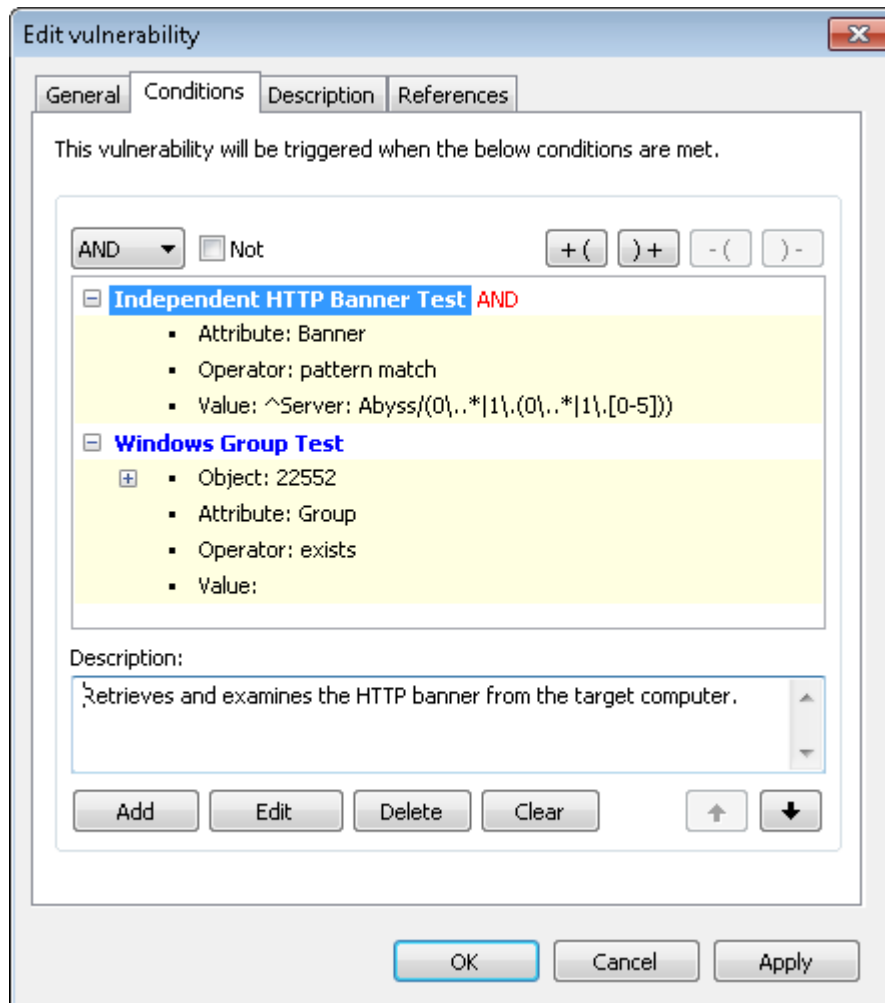
Table 48 - Vulnerability properties dialog

TAB NAME	DESCRIPTION
General	Use this tab to customize the general details of a vulnerability check including vulnerability check name, vulnerability type, OS family, OS version, Product, Timestamp and Severity.
Conditions	Use this tab to configure the operational parameters of this vulnerability check. These parameters will define whether a vulnerability check is successful or not. For information on how to configure vulnerability, check conditions refer to the Vulnerability check conditions setup section in this manual.
Description	Use this tab to customize the vulnerability check description.
References	Use this tab to customize references and links that lead to relevant information in the OVAL, CVE, MS Security, Security Focus and SANS TOP 20 reports.

3. Click on **OK** to save your settings.

Vulnerability check conditions setup

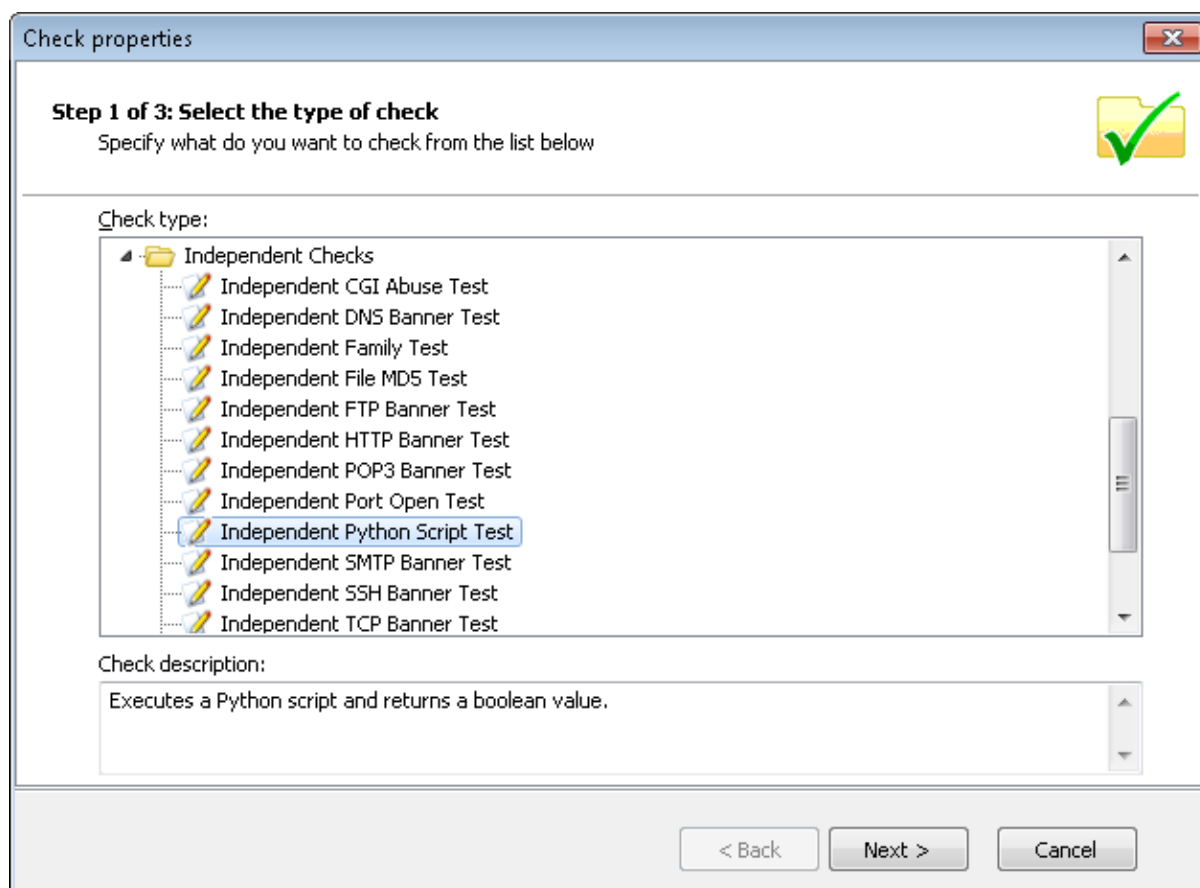
The **Conditions** tab enables you to add or customize conditions, which define whether the computer or network being scanned is vulnerable, or not. It is therefore of paramount importance that any custom checks defined in this section are set-up by qualified personnel that are aware of the ramifications of their actions.



Screenshot 117 - Vulnerability conditions setup tab

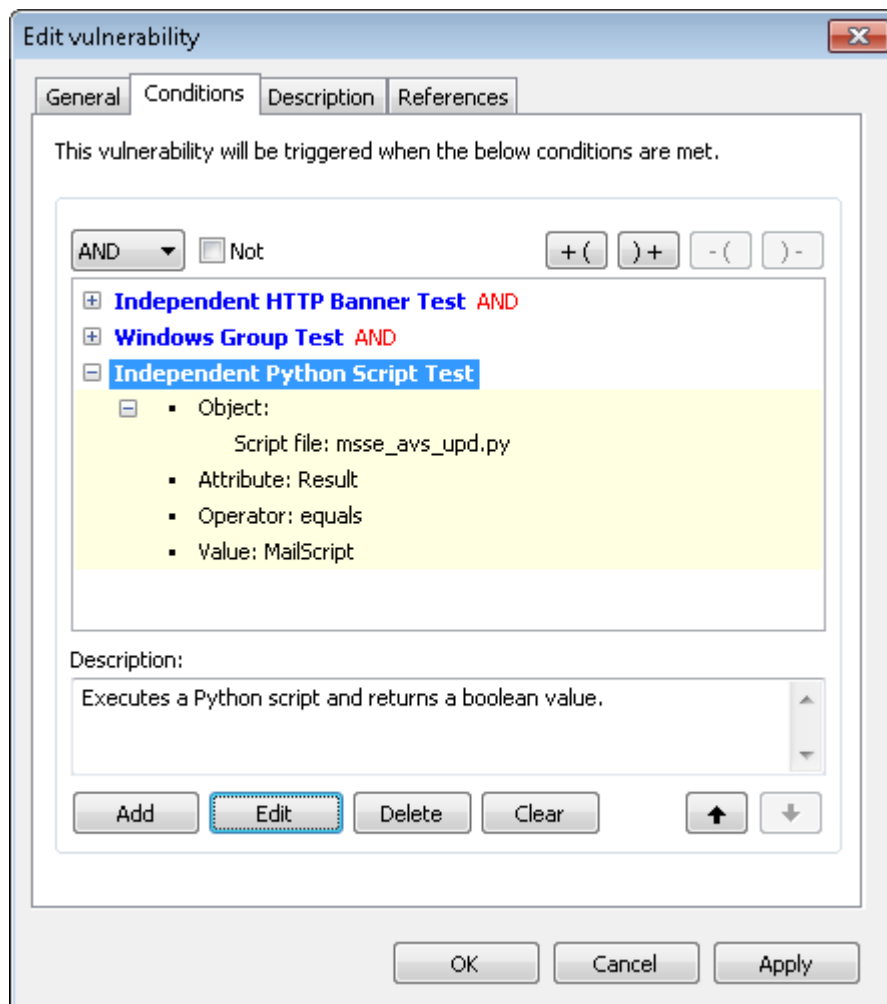
To add a vulnerability check condition:

1. Click **Add**.



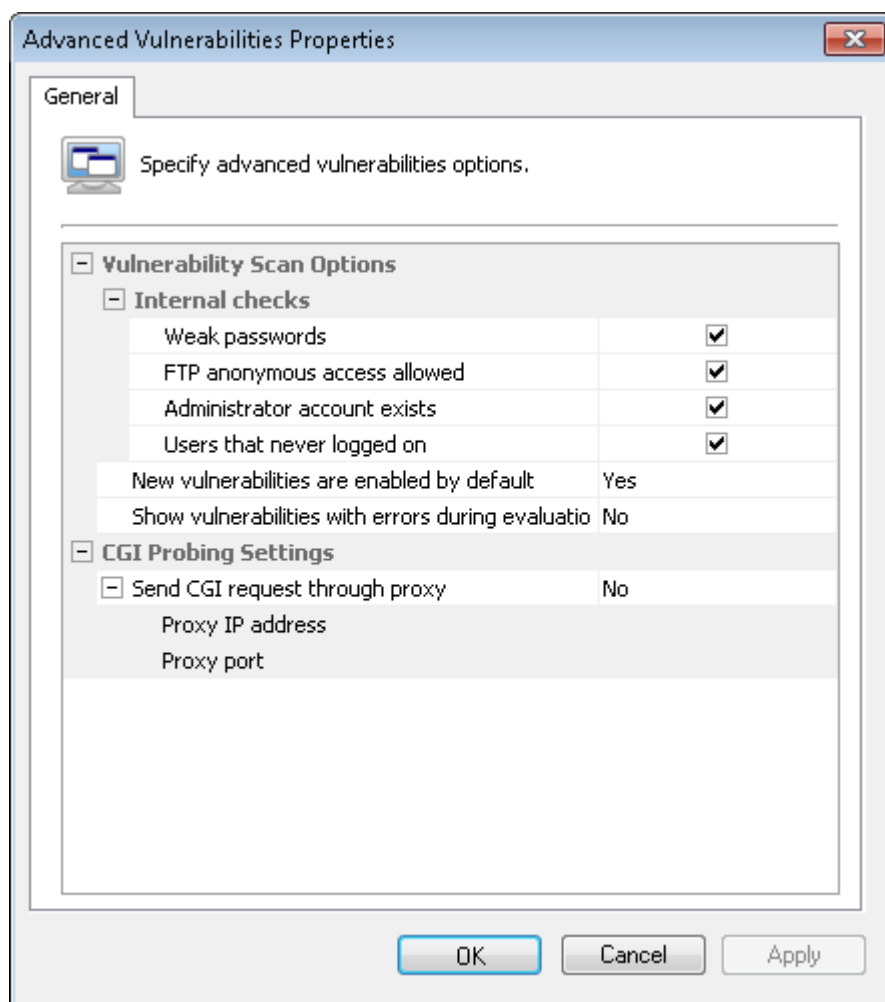
Screenshot 118 - Check properties wizard

2. Select the type of check to be configured and click **Next**.
3. Define the object to examine and click **Next**.
4. Set attributes/desired parameters and click **Finish** to finalize your settings.



Screenshot 119 - Edit vulnerability

5. If more than one condition is set up, define conditional operators and click **OK** to finalize your configuration settings.
6. (Optional) Click **Advanced...** in the **Vulnerabilities** tab to launch the advanced vulnerabilities scanning options.



Screenshot 120 - Advanced vulnerability scanning dialogs

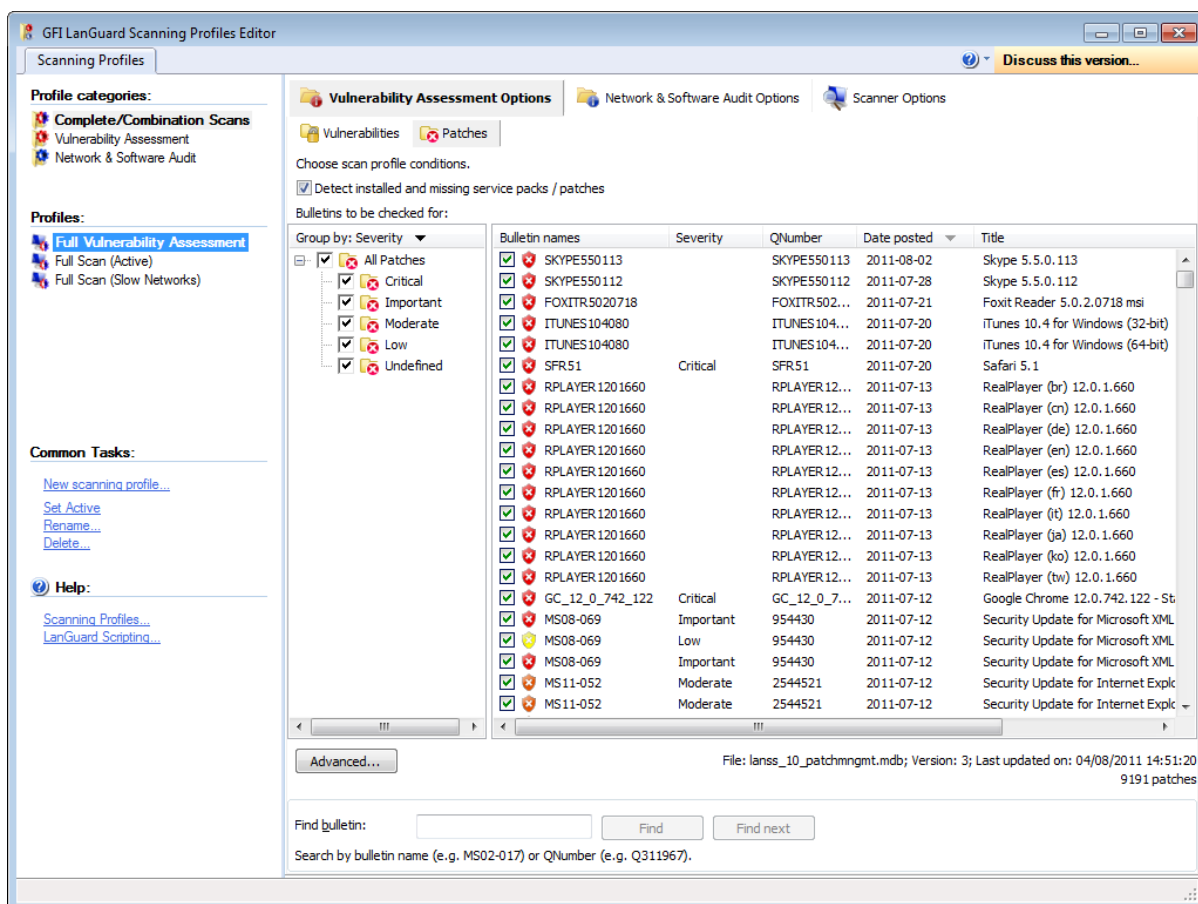
The options in Advanced Vulnerabilities Options are used to:

- » Configure extended vulnerability scanning features that check your target computers for weak passwords, anonymous FTP access, and unused user accounts.
- » Configure how GFI LanGuard handles newly created vulnerability checks.
- » Configure GFI LanGuard to send CGI requests through a specific proxy server. This is mandatory when CGI requests will be sent from a computer that is behind a firewall to a target web server that is 'outside' the firewall. For example, Web servers on a DMZ.

The firewall will generally block all the CGI requests that are directly sent by GFI LanGuard to a target computer that is in front of the firewall. To avoid this, set the **Send CGI requests through proxy** option to 'Yes' and specify the name/IP address of your proxy server and the communication port which will be used to convey the CGI request to the target.

8.3.2 Configuring patches

The **Patches** tab specifies the security updates checked during vulnerability scanning. The patches checked are selected from the complete list of supported software updates by default included in this tab. This list is automatically updated whenever GFI releases a new GFI LanGuard missing patch definition file.



Screenshot 121 - Scanning Profiles properties: Patches tab options

Enabling/disabling missing patch detection checks

To enable missing patch detection checks in a particular scanning profile:

1. From the **Vulnerability Assessment Options** tab, click **Patches** sub-tab.
2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
3. In the right pane, select **Detect installed and missing service packs/patches** option.



Missing patch scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable missing patch scanning in all profiles where missing patch scanning is required.

Customizing the list of software patches to be scanned

To specify which missing security updates will be enumerated and processed by a scanning profile:

1. From the **Vulnerability Assessment Options** tab, click **Patches** sub-tab
2. Select the scanning profile to customize from the left pane under **Profiles**.

Bulletin names	Severity	QNumber	Date posted	Title
☒  MS02-051	Moderate	324380	2005-02-19	Q324380: Security Update (Windows 2000)
☒  MS02-051	Moderate	324380	2005-03-25	Q324380: Security Update (Windows XP)
☒  MS04-008	Moderate	832359	2005-02-19	Security Update for Windows Media Services (KB832359)
☒  MS04-016	Moderate	839643	2004-06-10	Security Update for DirectX 8.0 (KB839643)
☒  MS04-016	Moderate	839643	2004-06-10	Security Update for DirectX 9.0 (KB839643)
☒  MS04-016	Moderate	839643	2004-06-11	Security Update for DirectX 8.1 (KB839643)
☒  MS04-016	Moderate	839643	2004-07-26	Security Update for Windows XP (KB839643)
☒  MS04-016	Moderate	839643	2004-12-15	Security Update for DirectX 9.0 (KB839643)
☒  MS04-016	Moderate	839643	2005-03-25	Security Update for Windows Server 2003 (KB839643)
☒  MS04-016	Moderate	839643	2005-09-12	Security Update for DirectX 8.2 (KB839643)
☒  MS04-016	Moderate	839643	2007-08-14	Security Update for DirectX 7.0 (KB839643)
☒  MS04-018	Moderate	823353	2006-04-11	Cumulative Security Update for Outlook Express 5.5 SP2 (KB823353)
☒  MS04-018	Moderate	823353	2006-04-11	Cumulative Security Update for Outlook Express 6 (KB823353)
☒  MS04-018	Moderate	823353	2006-04-11	Cumulative Security Update for Outlook Express 6 SP1 (KB823353)
☒  MS04-024	Moderate	839645	2005-02-17	Security Update for Windows Server 2003 (KB839645)
☒  MS04-028	Moderate	833989	2004-10-12	Security Update for Internet Explorer 6 Service Pack 1 (KB833989)
☒  MS05-006	Moderate	887981	2005-02-08	Security Update for Windows SharePoint Services (KB887981)
☒  MS05-009	Moderate	887472	2005-02-08	Security Update for Windows Messenger (KB887472)
☒  MS05-032	Moderate	890046	2007-05-08	Security Update for Windows Server 2003 (KB890046)
☒  MS05-032	Moderate	890046	2007-05-08	Security Update for Windows Server 2003 64-bit Itanium Edition (KB...
☒  MS05-032	Moderate	890046	2007-05-08	Security Update for Windows Server 2003 x64 Edition (KB890046)
☒  MS05-032	Moderate	890046	2007-05-08	Security Update for Windows XP (KB890046)
☒  MS05-032	Moderate	890046	2007-05-08	Security Update for Windows XP x64 Edition (KB890046)

Screenshot 122 - Select the missing patches to enumerate

3. In the right pane, select/unselect which missing patches are enumerated by this scanning profile.

Searching for bulletin information

Find bulletin:

Find

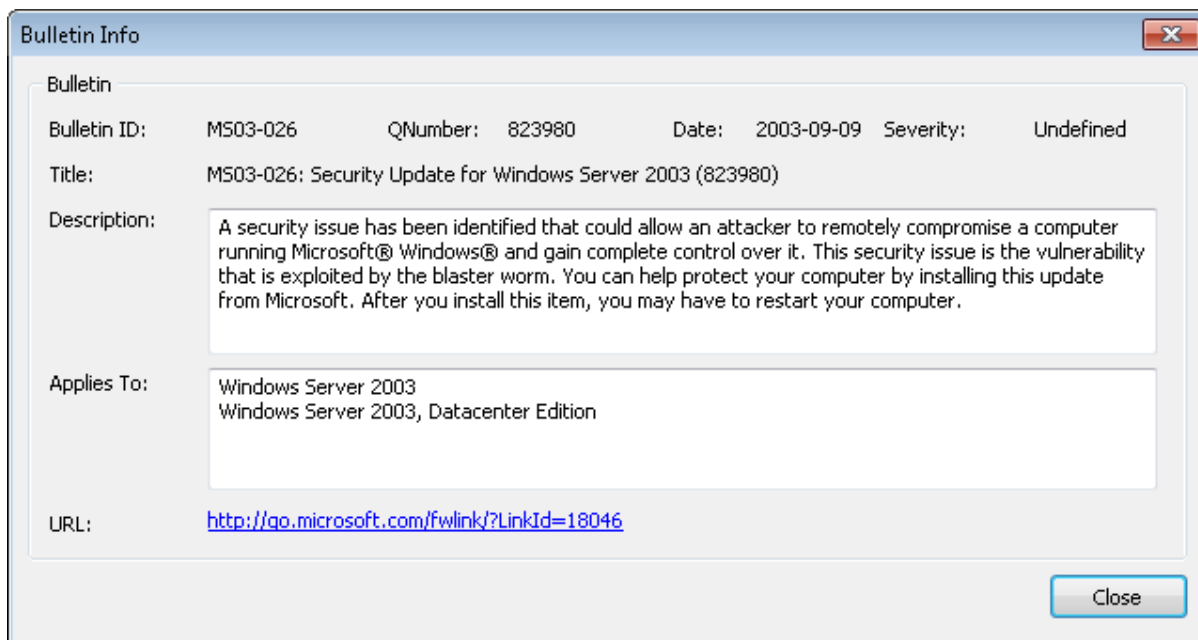
Find next

Search by bulletin name (e.g. MS02-017) or QNumber (e.g. Q311967).

Screenshot 123 - Searching for bulletin information

To search for a particular bulletin:

1. From **Vulnerability Assessment Options** ► **Vulnerabilities** ► **Find bulletin:**, specify the bulletin name (for example, MS02-017) or QNumber (for example, Q311987) in the search tool entry box included at the bottom of the right pane.
2. Click **Find** to search for your entry.

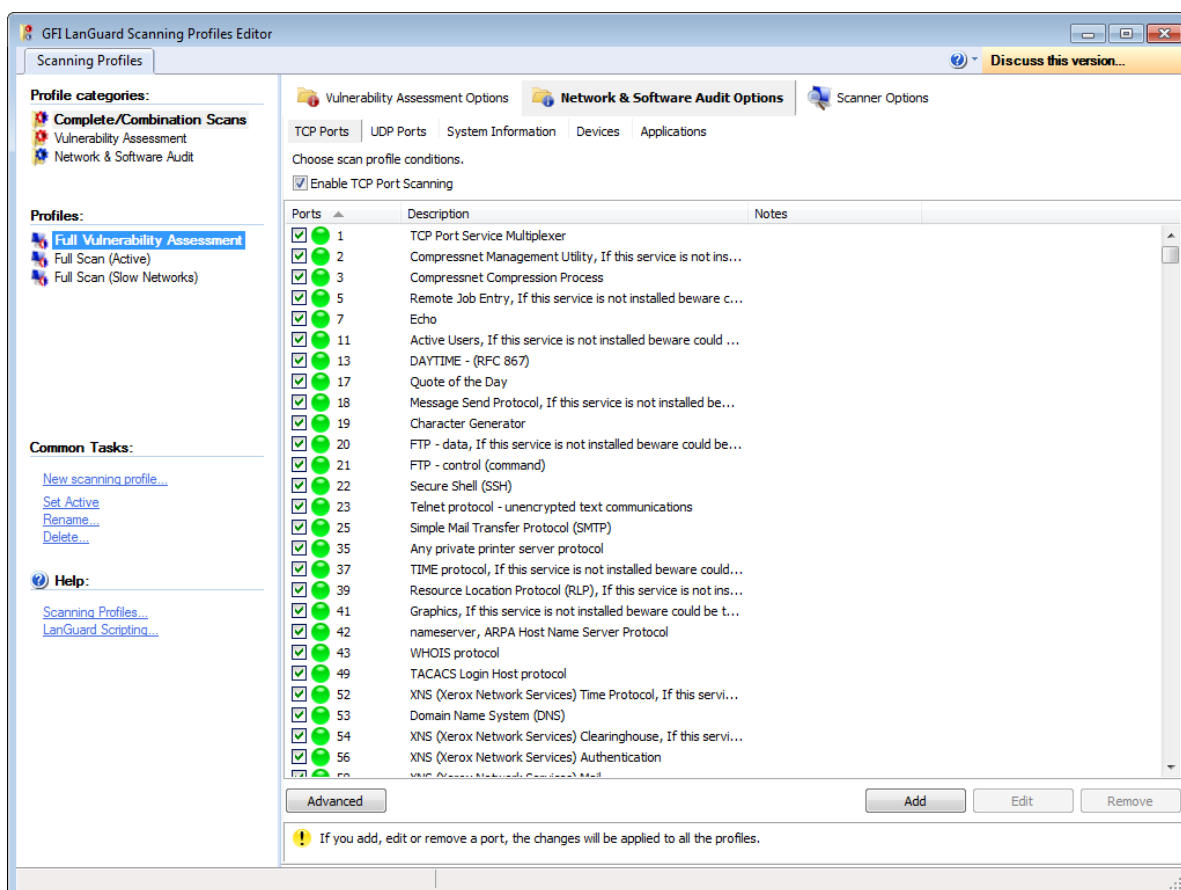


Screenshot 124 - Extended bulletin information

8.4 Configure Network & Software Audit options

The scanning profiles that ship with GFI LanGuard are already pre-configured to run a number of network and software audit checks on selected target. You can however disable scanning as well as customize the list of network and software audits executed during a scan.

8.4.1 Configuring TCP port scanning options



Screenshot 125 - Scanning Profiles properties: TCP Ports tab options

Enabling/disabling TCP Port scanning

To enable TCP Port Scanning in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub-tab.
2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
3. Select **Enable TCP Port Scanning** option.

Configuring the list of TCP ports to be scanned

To configure which TCP ports will be processed by a scanning profile:

1. From **Network & Security Audit Options** tab, click **TCP Ports** sub-tab.
2. Select scanning profile to customize from the left pane under **Profiles**.
3. Select TCP ports to analyze with this scanning profile.

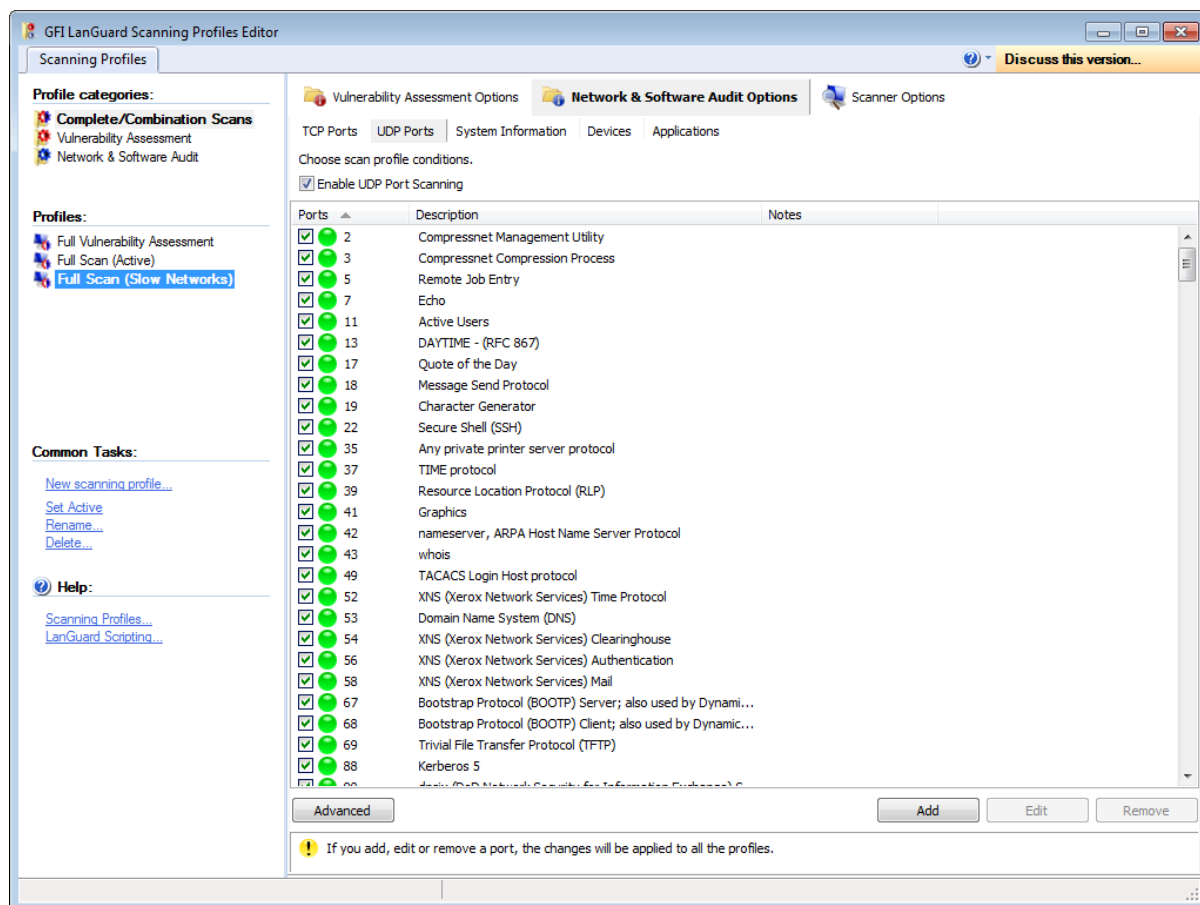
Customizing the list TCP ports

1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub-tab.
2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
3. Customize the list of TCP Ports through **Add**, **Edit** or **Remove**.



The list of supported TCP/UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles

8.4.2 Configuring UDP port scanning options



Screenshot 126 - Scanning Profiles properties: UDP Ports tab options

Enabling/disabling UDP Port scanning

To enable UDP Port Scanning in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click **UDP Ports** sub-tab.
2. Select scanning profile to customize from the left pane under **Profiles**.
3. Select **Enable UDP Port Scanning** option.

Configuring the list of UDP ports to be scanned

To configure the UDP ports to process, select the required ports:

1. From the **Network & Security Audit Options** tab, click **UDP Ports** sub-tab.
2. Select the scanning profile to customize from the left pane under **Profiles**.
3. Select the UDP ports that will be analyzed by this scanning profile.

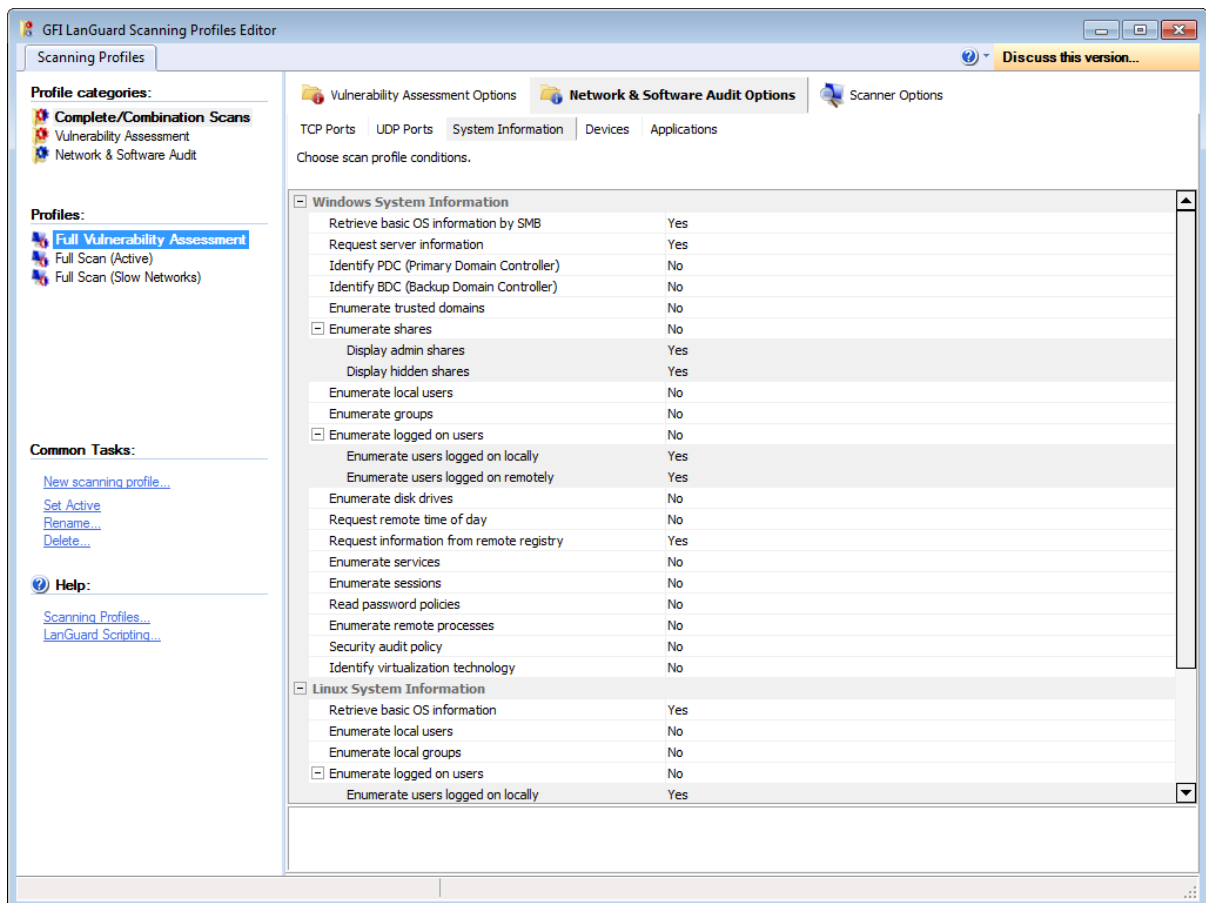
Customizing the UDP ports list

1. From the **Network & Security Audit Options** tab, click **UDP Ports** sub-tab.
2. Select the scanning profile to customize from the left pane under **Profiles**.
3. Customize the list of UDP Ports through **Add**, **Edit** or **Remove**.



The list of supported UDP ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles.

8.4.3 Configuring System Information options



Screenshot 127 - Scanning Profiles properties: System Information tab options

To specify what System Information is enumerated by a particular scanning profile:

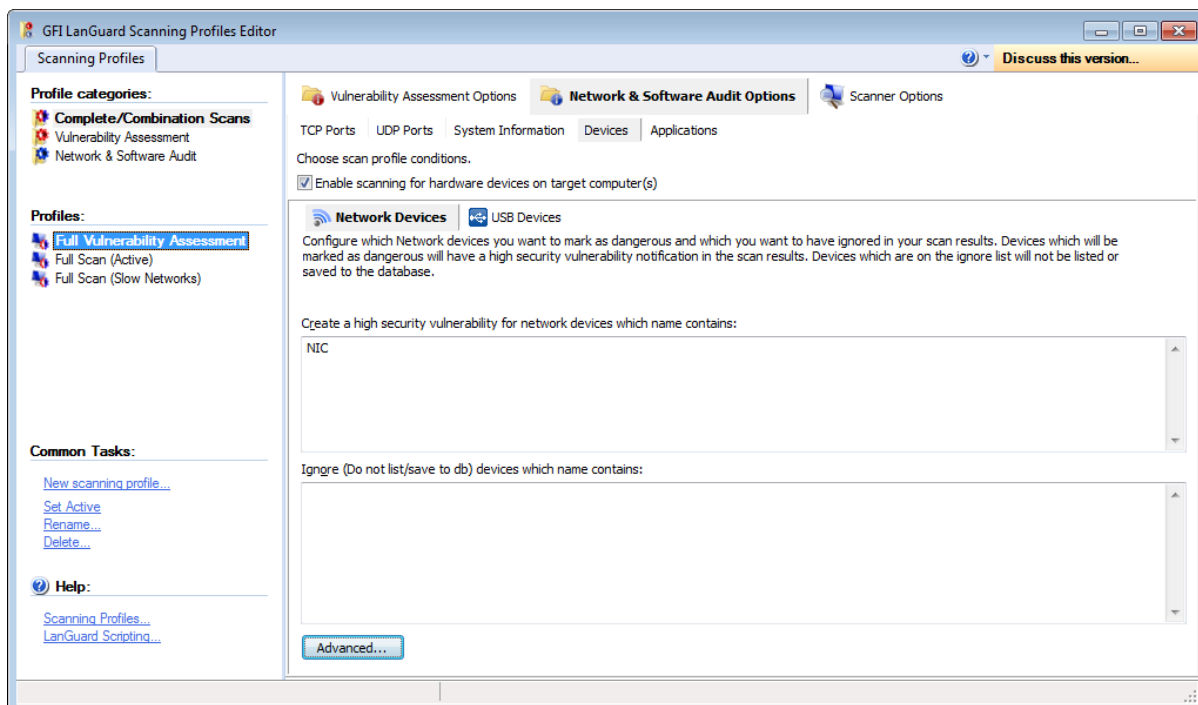
1. From the **Network & Security Audit Options** tab, click **System Information** sub-tab.
2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
3. From the right pane, expand the **Windows System Information** group or **Linux System Information** group accordingly.
4. Select which Windows/Linux OS information is retrieved by the security scanner from scanned targets.

For example, to enumerate administrative shares in scan results, expand the **Enumerate shares** option and set the **Display admin shares** option to 'Yes'.

8.4.4 Configuring Devices scanning options

Use the **Devices** tab to enumerate network devices. Together with device enumeration, you can further configure GFI LanGuard to generate high security vulnerability alerts whenever a USB or Network device is detected.

This is achieved by compiling a list of unauthorized/blacklisted Network and USB devices that you want to be alerted.



Screenshot 128 - The network devices configuration page

GFI LanGuard can also exclude from the scanning process specific USB devices that you consider safe. Such devices can be a USB mouse or keyboard. This is achieved through a safe/white list of USB devices to ignored during scanning.

Similarly you can create a separate scanning profile that enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers. In this case however, you must specify 'Bluetooth' and 'Wireless' or 'WiFi' in the unauthorized network and USB lists of your scanning profile.

All the device scanning configuration options are accessible through the two sub-tabs contained in the devices configuration page. These are the **Network Devices** tab and the **USB Devices** tab.

Use the **Network Devices** sub-tab to configure the attached network devices scanning options and blacklisted (unauthorized)/white-listed (safe) devices lists.

Use the **USB Devices** sub-tab to configure the attached USB devices scanning options and unauthorized/safe devices lists.

Enabling/disabling checks for all installed network devices

To enable network device (including USB device) scanning in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab
2. Click **Network Devices** tab
3. Select the scanning profile to customize from the left pane under **Profiles**.
4. From the right pane, select **Enable scanning for hardware devices on target computer(s)**.



Network device scanning is configurable on a scan profile by scan profile basis. Make sure to enable network device scanning in all profiles where this is required.

Compiling a network device blacklist/white-list

To compile a network device blacklist/white-list for a scanning profile:

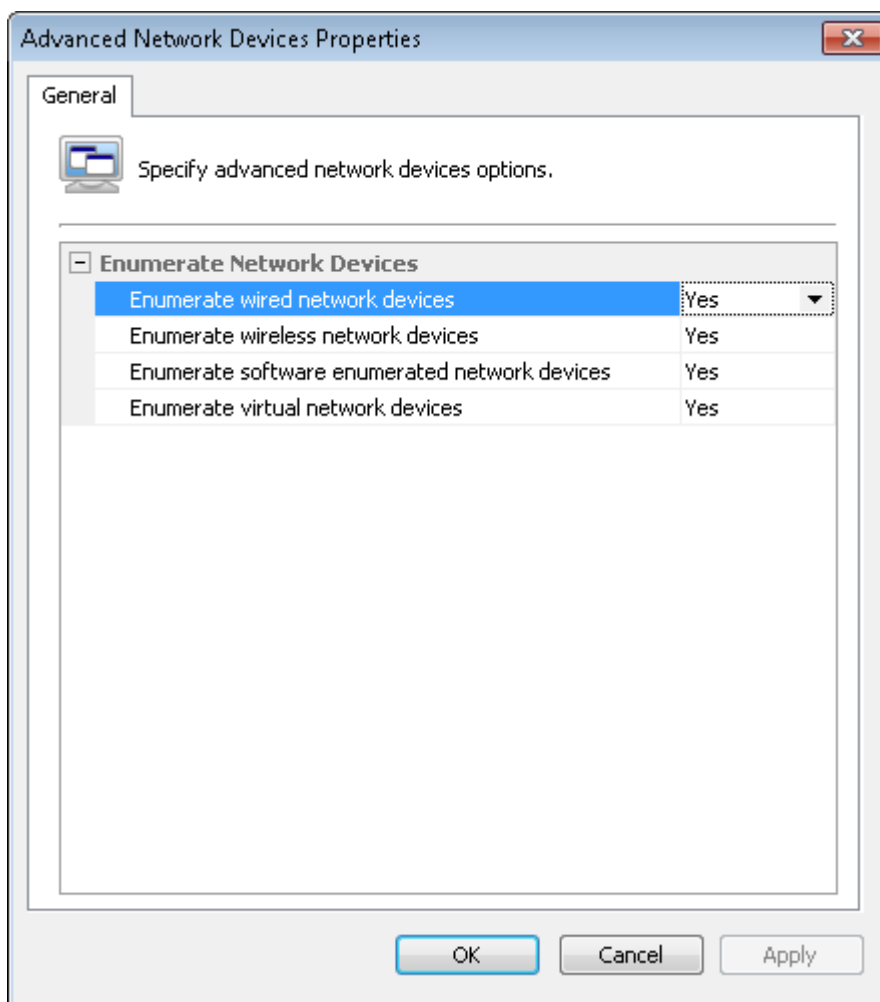
1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab.
2. Click **Network Devices** tab.
3. Select the scanning profile to customize from the left pane under **Profiles**.
4. In the right pane: to create a network device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under **Create a high security vulnerability for network devices which name contains**.

For example, if you enter the word 'wireless' you will be notified through a high security vulnerability alert when a device whose name contains the word 'wireless' is detected. To create a network device white-list, specify which devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db) devices which name contains**.



Only include one network device name per line.

Configuring advanced network device scanning options



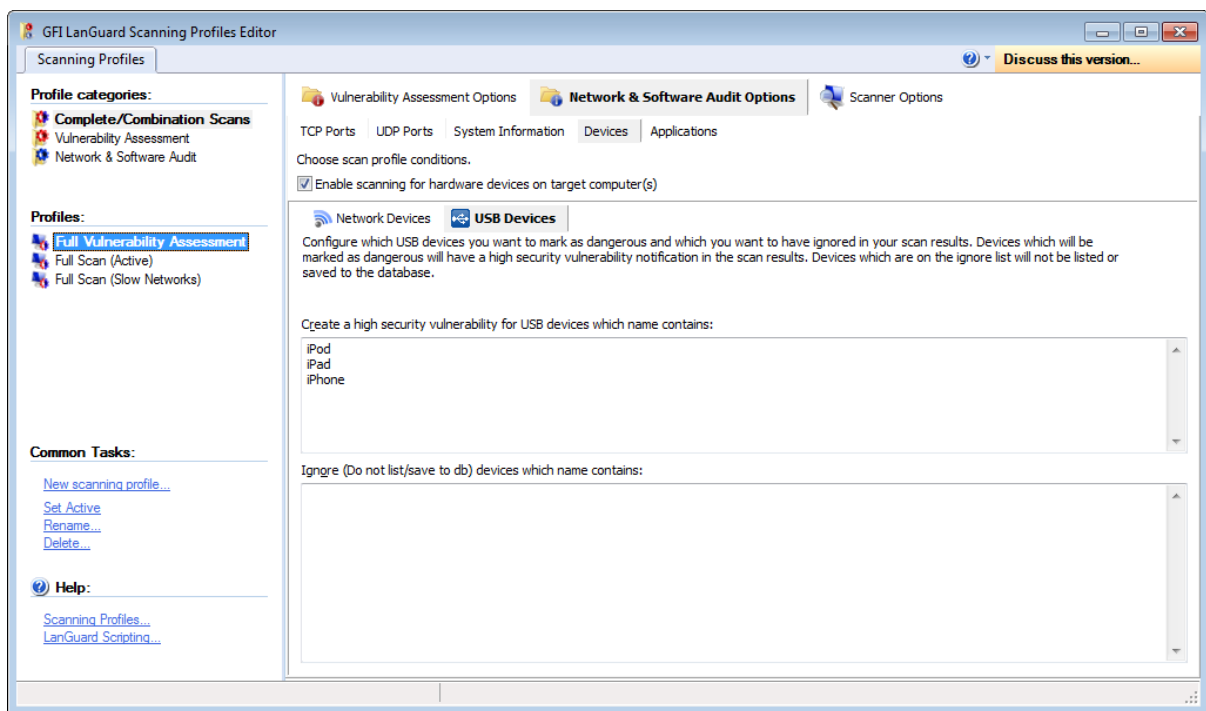
Screenshot 129 - Advanced network devices configuration dialog

From the **Network Devices** tab, you can also specify the type of network devices checked by this scanning profile and reported in the scan results. These include ‘wired network devices’, ‘wireless network devices’, ‘software enumerated network devices’ and ‘virtual network devices’.

To specify which network devices to enumerate in the scan results:

1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab.
2. Click on the **Network Devices** tab (opens by default).
3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
4. Click **Advanced** at the bottom of the page.
5. Set the required options to **Yes**. Click **OK** to finalize your settings.

Scanning for USB devices



Screenshot 130 - The Devices configuration page: USB Devices tab options

To compile a list of unauthorized/unsafe USB devices:

1. From the **Network & Security Audit Options** tab, click the **Devices** sub-tab.
2. Click **USB Devices** tab.
3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
4. In the right pane, specify which devices you want to classify as high security vulnerabilities in the space provided under **Create high security vulnerability for USB devices which name contains:**.

For example, if you enter the word ‘iPod’, you will be notified through a high security vulnerability alert when a USB device whose name contains the word ‘iPod’ is detected.

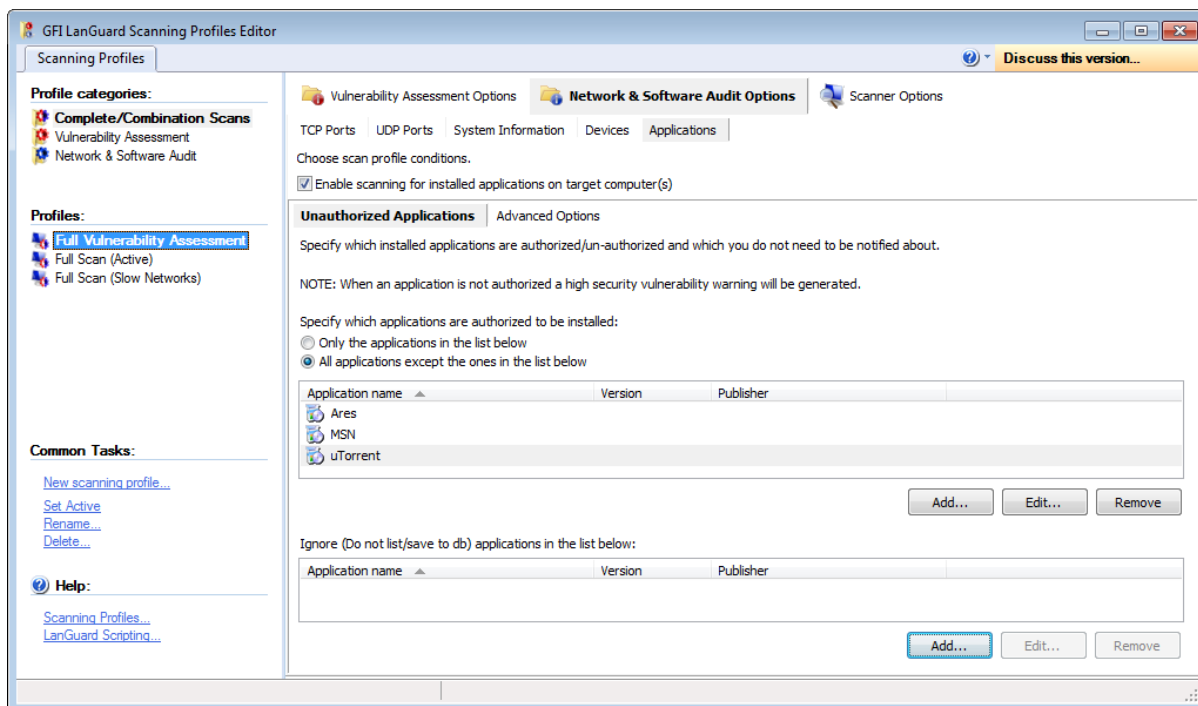
To create a USB device white-list, specify which USB devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db) devices which name contains**.



Only include one USB device name per line.

8.4.5 Configuring applications scanning options

The **Applications** tab enables you to specify which applications will trigger an alert during a scan.



Screenshot 131 - The applications configuration page

Through this tab, you can also configure GFI LanGuard to detect and report unauthorized software installed on scanned targets and to generate high security vulnerability alerts whenever such software is detected.

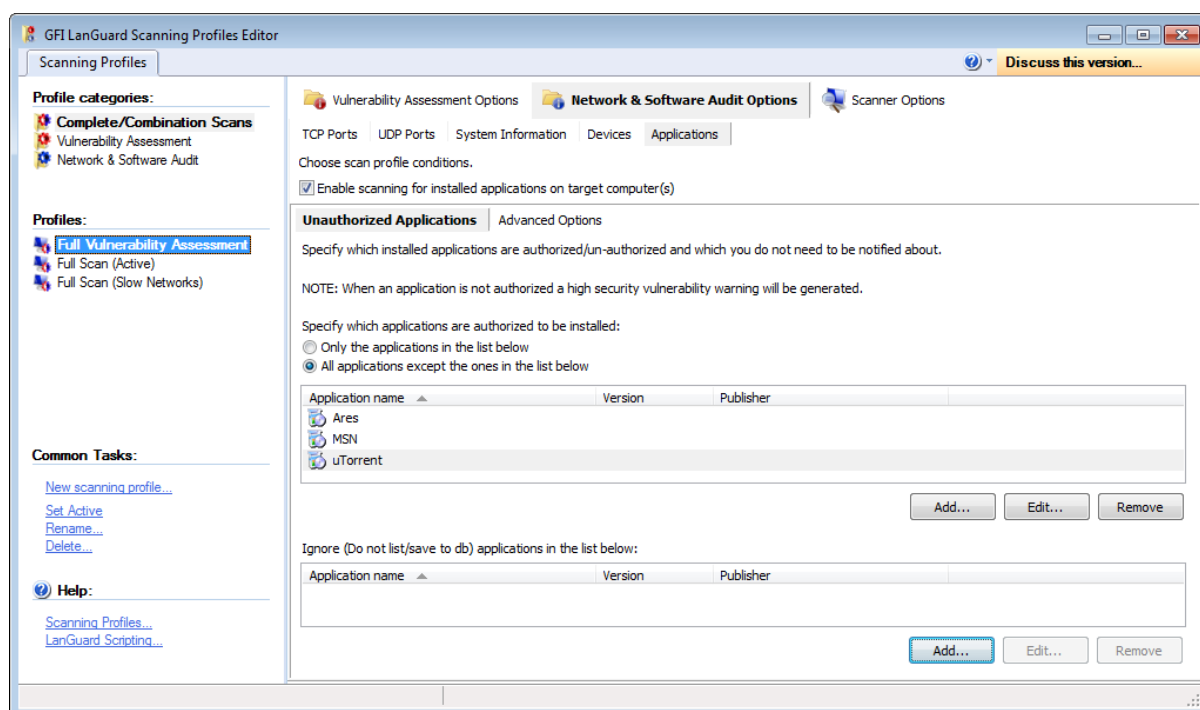
Scanning installed applications

By default, GFI LanGuard also supports integration with particular security applications. These include various anti-virus and anti-spyware software.

During security scanning, GFI LanGuard checks the correct configuration of virus scanner(s) or anti-spyware software and that the respective definition files are up to date.

Application scanning is configurable on a scan profile by scan profile basis and all the configuration options are accessible through the two sub-tabs contained in the **Applications** tab. These are the **Unauthorized Applications** sub-tab and the **Advanced Options** sub-tab.

Enabling/disabling checks for installed applications



Screenshot 132 - The Applications tab: Installed Applications tab options

To enable installed applications scanning in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab.
2. Click on the **Unauthorized Applications** sub-tab.
3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
4. Select the **Enable scanning for installed applications on target computer(s)** checkbox.



Installed applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable installed applications scanning in all profiles where this is required.

Compiling installed applications blacklist/white-list

To compile installed applications blacklist/white-list:

1. From the **Network & Security Audit Options** tab, click **Applications** sub-tab.
2. Select **Unauthorized Applications** sub-tab.
3. Select the scanning profile to customize from the left pane under **Profiles**.
4. From the right pane, select **Enable scanning for installed applications on target computer(s)** checkbox.
5. Specify the applications that are authorized for installation. Table 49 below describes the available options:

Table 49 - Applications Options

OPTION	DESCRIPTION
Only the applications in the list below	Specify names of applications that are authorized for installation. These applications will be ignored during a security scan.

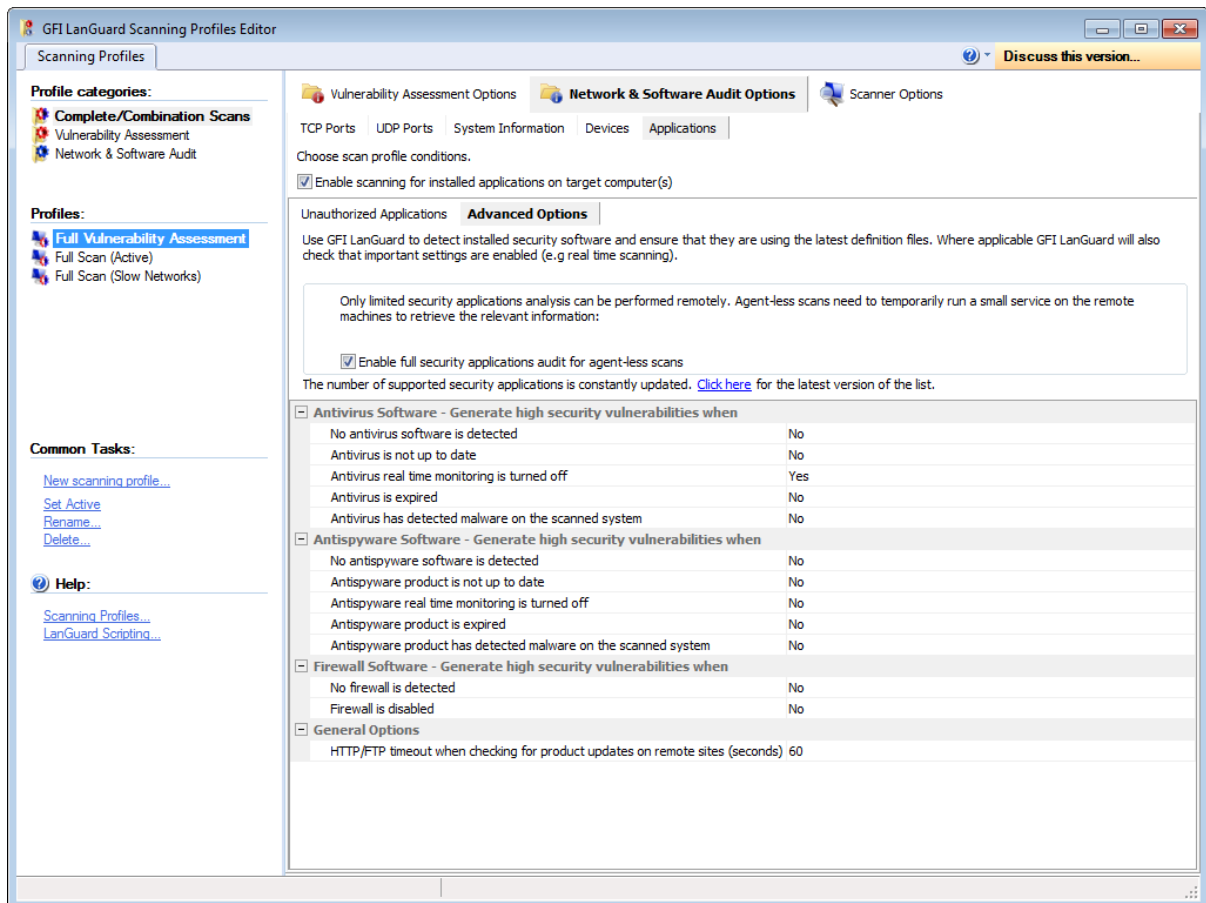
OPTION	DESCRIPTION
All applications except the ones in the list below	Specify the names of the applications that are unauthorized for installation. Applications not in this list will be ignored during a security scan.

6. In the **Ignore (Do not list/save to db) applications from the list below** options key in applications by clicking **Add**. Any application listed is white-listed.



Include only one application name per line.

Advanced application scanning options



Screenshot 133 -The Applications configuration page: Advanced Options

GFI LanGuard ships with a default list of anti-virus and anti-spyware applications that can be checked during security scanning.

The **Advanced Options** tab enables you to configure when GFI LanGuard will generate high security vulnerability alerts if it detects certain configurations of a security application.

Alerts are generated when:

- » No anti-virus, anti-spyware or firewall is detected
- » A fake anti-virus or anti-spyware is detected
- » Anti-virus or anti-spyware definitions are not up to date
- » Anti-virus or anti-spyware real-time monitoring is turned off
- » Anti-virus or anti-spyware product is expired

- » Anti-virus or anti-spyware product detects malware on the scanned computer(s)
- » Firewall is disabled
- » HTTP/FTP timeout when checking for product updates on remote sites. This option generates an alert if the number of seconds defined for timeout is exceeded.

Enabling/disabling checks for security applications

To enable checks for installed security applications in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab.
2. Click on the **Advanced Options** tab.
3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
4. Select **Enable scanning for installed applications on target computer(s)** checkbox.
5. (Agent-less scans) Select **Enable full security applications audit for agent-less scans** checkbox.



Agent-less scans temporarily runs a small service on the remote computers in order to retrieve the relevant information.



Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.



The number of supported security applications is constantly updated. Click the link available in order to get the latest version of the list. Configuring security applications - advanced options

To configure alerting triggers for installed security applications in a particular scanning profile:

1. From **Network & Security Audit Options** tab, click **Applications** sub-tab.
2. Click **Advanced Options** tab.
3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.
4. Select **Enable scanning for installed applications on target computer(s)** checkbox.
5. (Agent-less scans) Select **Enable full security applications audit for agent-less scans** checkbox.

[-] Antivirus Software - Generate high security vulnerabilities when	
No antivirus software is detected	No
Antivirus is not up to date	Yes
Antivirus real time monitoring is turned off	No
Antivirus is expired	Yes
Antivirus has detected malware on the scanned system	Yes
[-] Antispyware Software - Generate high security vulnerabilities when	
No antispyware software is detected	Yes
Antispyware product is not up to date	Yes
Antispyware real time monitoring is turned off	Yes
Antispyware product is expired	Yes
Antispyware product has detected malware on the scanned system	Yes
[-] Firewall Software - Generate high security vulnerabilities when	
No firewall is detected	Yes
Firewall is disabled	Yes
[-] General Options	
HTTP/FTP timeout when checking for product updates on remote sites (seconds)	60

Screenshot 134 - Security Applications Alert Configuration

6. From the bottom-right pane, select the trigger you want to configure and choose between **Yes** or **No** from the drop down menu next to the respective alert trigger.

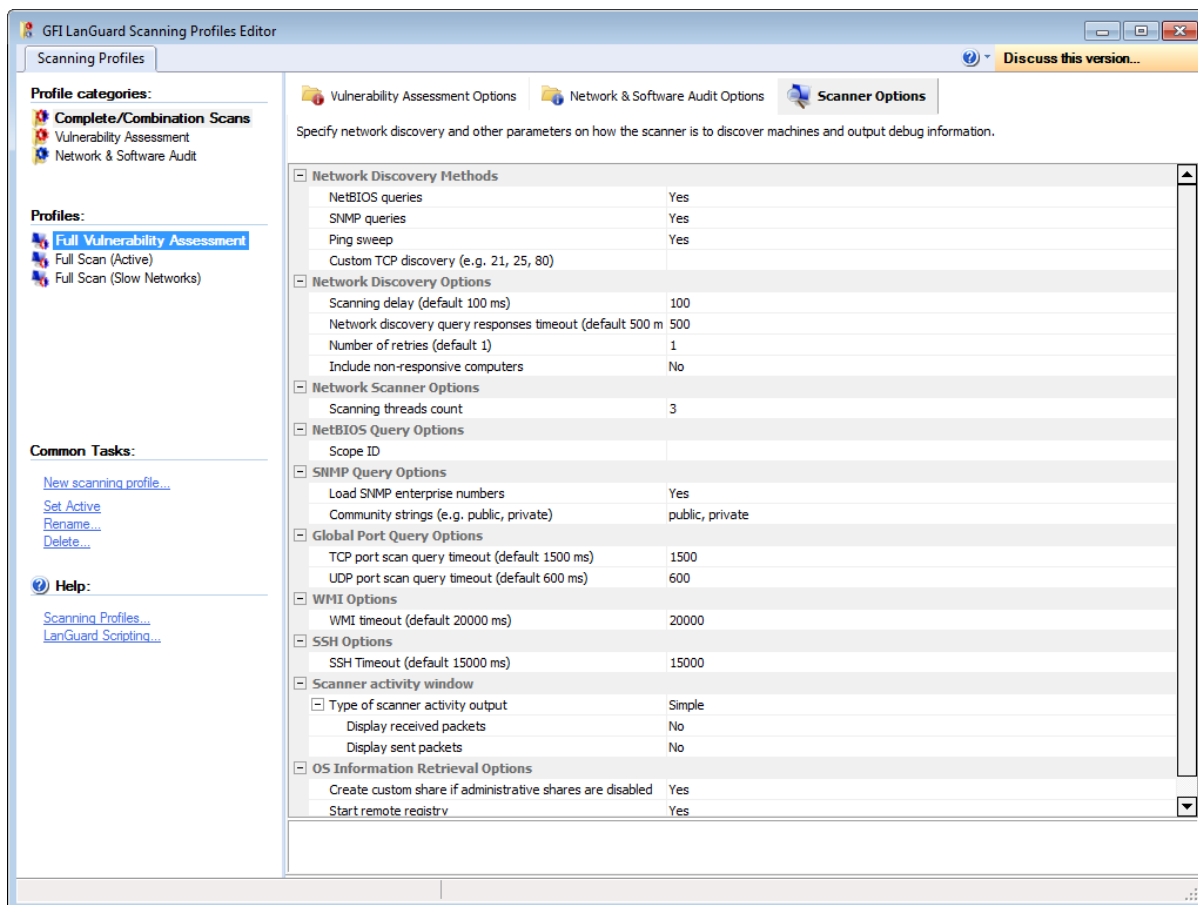


Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.

8.5 Configuring the security scanning options

Use **Scanner Options** tab to configure the operational parameters of the security-scanning engine.

These parameters are configurable on a scan profile by scan profile basis and define how the scanning engine will perform target discovery and OS Data querying.



Screenshot 135 - Scanning Profiles properties: Scanner Options tab

Configurable options include timeouts, types of queries to run during target discovery, number of scanning threads count, SNMP scopes for queries and more.



Configure these parameters with extreme care! An incorrect configuration can affect the security scanning performance of GFI LanGuard.

9 Utilities

9.1 Introduction

Use the **Utilities** tab to access the following list of default network tools:

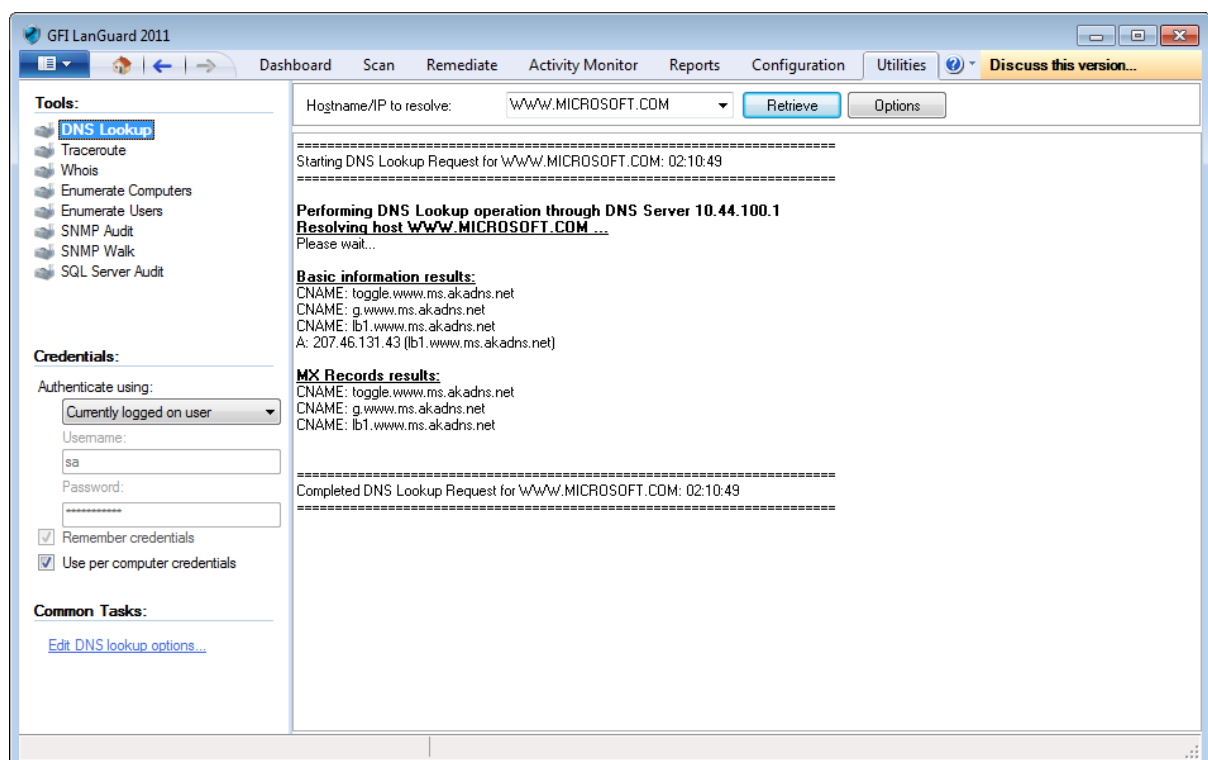
- » **DNS Lookup**
- » **Traceroute**
- » **Whois**
- » **Enumerate Computers**
- » **Enumerate Users**
- » **SNMP Audit**
- » **SNMP Walk**
- » **SQL Server Audit**

9.2 DNS lookup

DNS lookup resolves domain names into the corresponding IP address and retrieves particular information from the target domain (for example, MX record, etc.).

To resolve a domain/host name:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **DNS Lookup** in the left pane under **Tools**.
3. Specify the hostname to resolve in the **Hostname/IP to resolve** textbox.



Screenshot 136 - The DNS Lookup tool

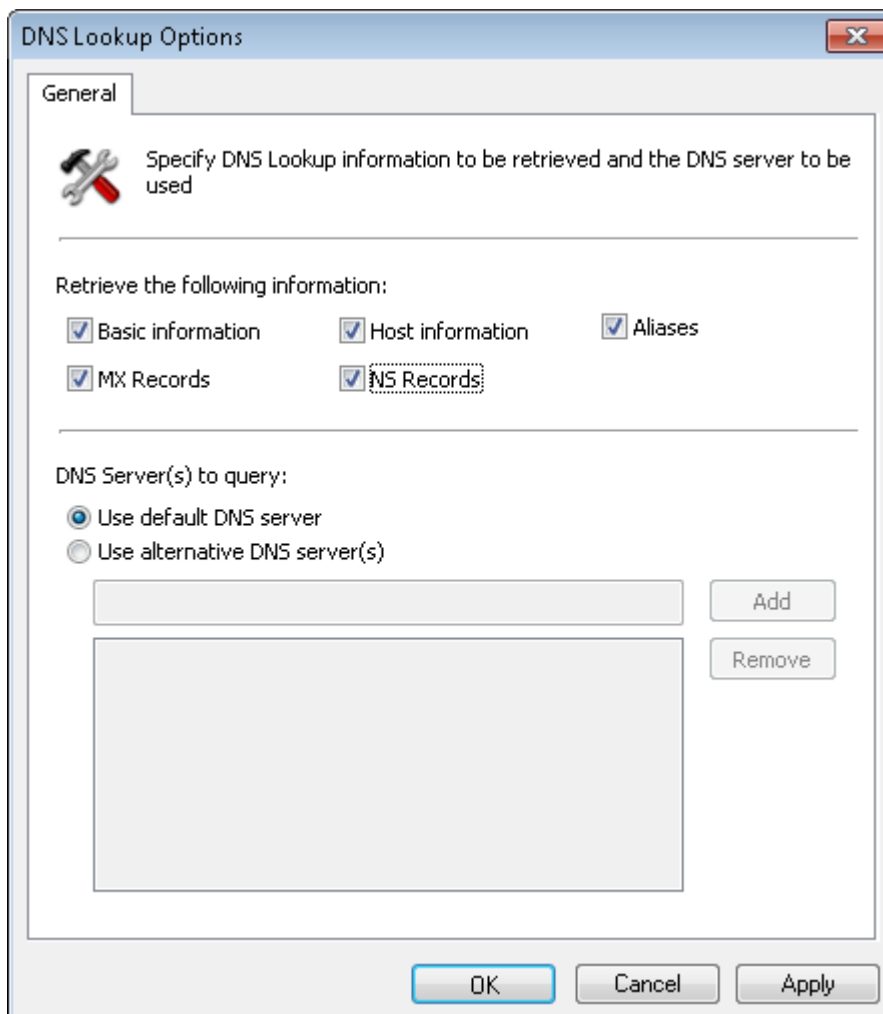
4. Under **Common Tasks** in the left pane, click on **Edit DNS Lookup options...** or click **Options** on the right pane and specify the information described in Table 50 below:

Table 50 -DNS lookup options

OPTION	DESCRIPTION
Basic Information	Retrieve the host name and the relative IP address.
Host Information	Retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.
Aliases	Retrieve information on the 'A Records' configured on the target domain.
MX Records	Enumerate all the mail servers and the order (i.e. priority) in which they receive and process emails for the target domain.
NS Records	Specify the 'name-servers' that are authoritative for a particular domain or sub domain.



Some DNS entries do not contain certain information for security reasons.



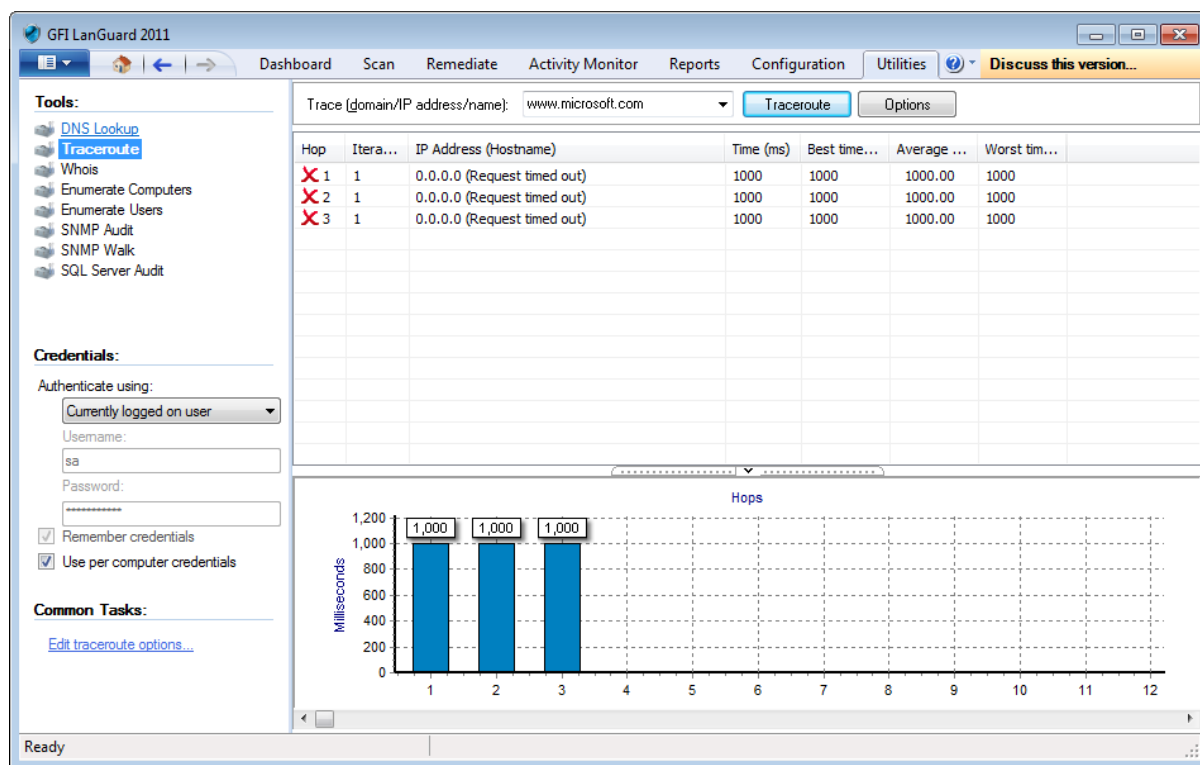
Screenshot 137 - The DNS Lookup tool

5. (Optional) Specify the alternative DNS server that will be queried by the DNS Lookup tool or leave as default to use the default DNS server.

6. Click **Retrieve** to start the process.

9.3 Traceroute

Traceroute identifies the path that GFI LanGuard followed to reach a target computer.



Screenshot 138 - Trace route tool

To use the traceroute tool:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **Traceroute** in the left pane under **Tools**.
3. In the **Trace (domain/IP/name)** dropdown, specify the name/IP or domain to reach.
4. (Optional) Under **Common Tasks** in the left pane, click on **Edit Traceroute options...** or click **Options** on the right pane to change the default options.
5. Click on the **Traceroute** button to start the tracing process.

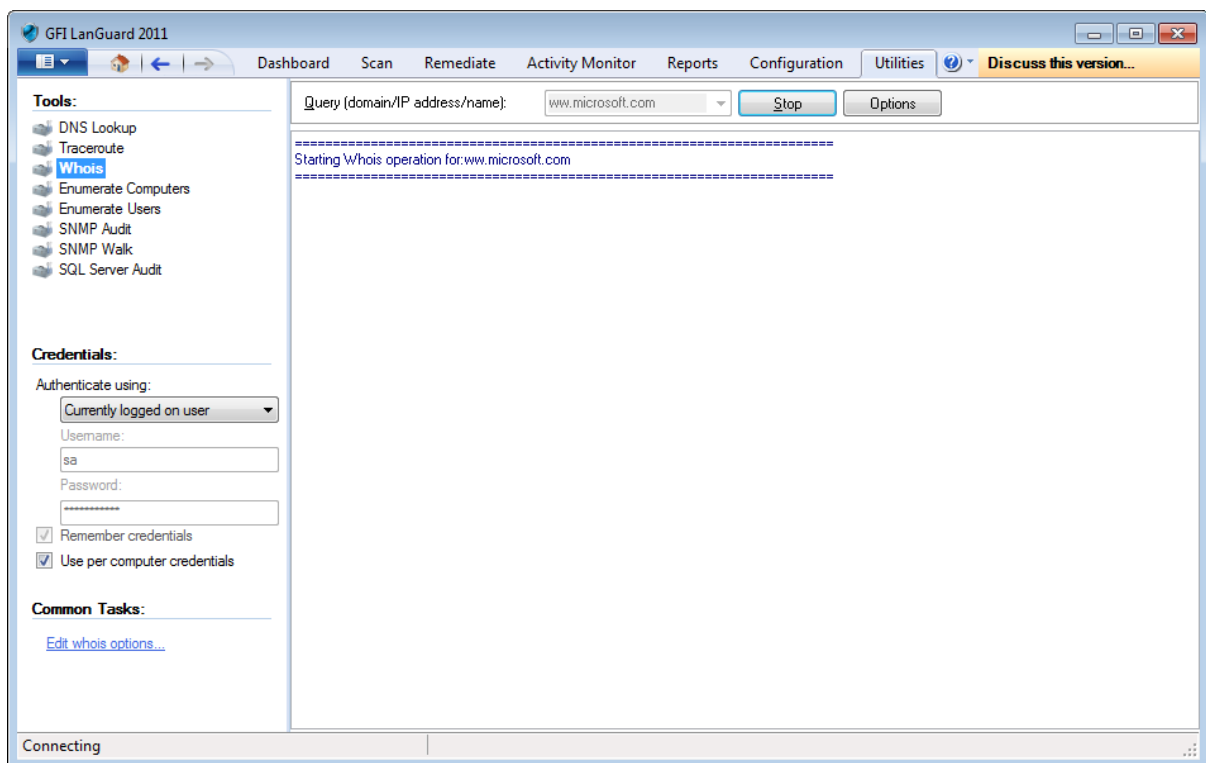
Traceroute will break down, the path taken to a target computer into 'hops'. A hop indicates a stage and represents a computer that was traversed during the process.

The information enumerated by this tool includes the IP of traversed computers, the number of times that a computer was traversed and the time taken to reach the respective computer. An icon is also included next to each hop. This icon indicates the state of that particular hop. The icons used in this tool include:

- ✓ Indicates a successful hop taken within normal parameters.
- ⚠ Indicates a successful hop, but time required was quite long.
- ⚠ Indicates a successful hop, but the time required was too long.
- ✗ Indicates that the hop was timed out (> 1000ms).

9.4 Whois

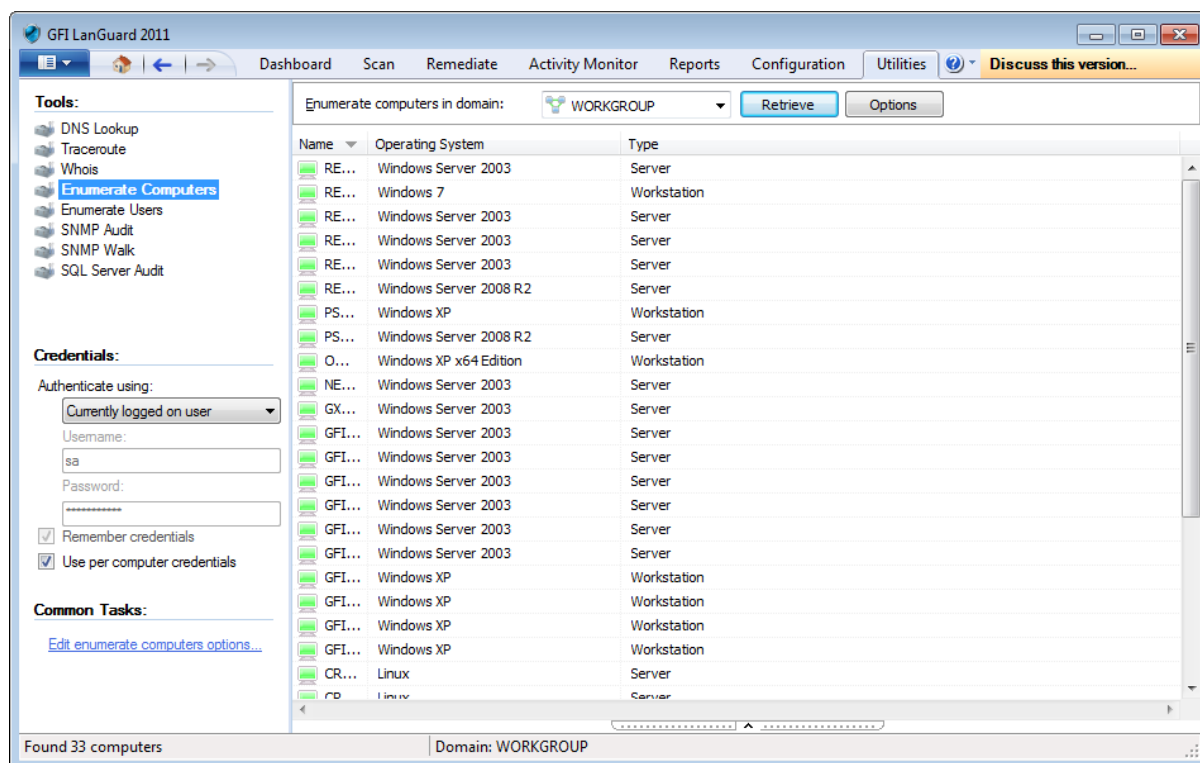
Whois looks up information on a particular domain or IP address.



Screenshot 139 - Whois tool

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **Whois** in the left pane under **Tools**.
3. In **Query (domain/IP/name)** dropdown menu, specify the name/IP or domain to reach.
4. (Optional) From **Common Tasks** in the left pane, click **Edit Whois options...** or **Options** on the right pane to change the default options.
5. Click **Retrieve** to start the process.

9.5 Enumerate computers



Screenshot 140 - Enumerate Computers tool

The enumerate computers utility identifies domains and workgroups on a network. During execution, this tool will also scan each domain/workgroup discovered so to enumerate their respective computers.

The information enumerated by this tool includes:

- » The domain or workgroup name
- » The list of domain/workgroup computers
- » The operating system installed on the discovered computers
- » Any additional details that might be collected through NetBIOS

Computers are enumerated using one of the following methods:

- » **From Active Directory** - This method is much faster and will include computers that are currently switched off.
- » **From Windows Explorer** - This method enumerates computers through a real-time network scan and therefore it is slower and will not include computers that are switched off.

To enumerate computers:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **Enumerate Computers** in the left pane under **Tools**.
3. In the **Enumerate computers in domain** dropdown, select the desired domain.
4. From **Common Tasks** in the left pane, click **Edit Enumerate Computers options...** or **Options** on the right pane.

5. Select whether to enumerate computers from Active Directory or Windows Explorer.
6. Click **Retrieve** to start the process.



For an Active Directory scan, you will need to run the tool under an account that has access rights to the Active Directory

9.5.1 Starting a security scan

The **Enumerate Computers** tool scans your entire network and identifies domains and workgroups as well as their respective computers. After enumerating the computers in a domain or workgroup, you can use this tool to launch a security scan on the listed computers.

To start a security scan directly from the 'Enumerate Computers' tool, right-click on any of the enumerated computers and select **Scan**.

You can also launch a security scan and at the same time continue using the **Enumerate Computers** tool. This is achieved by right-clicking on any of the enumerated computers and selecting **Scan in background**.

9.5.2 Deploying custom patches

You can use the **Enumerate Computers** tool to deploy custom patches and third party software on the enumerated computers. To launch a deployment process directly from this tool:

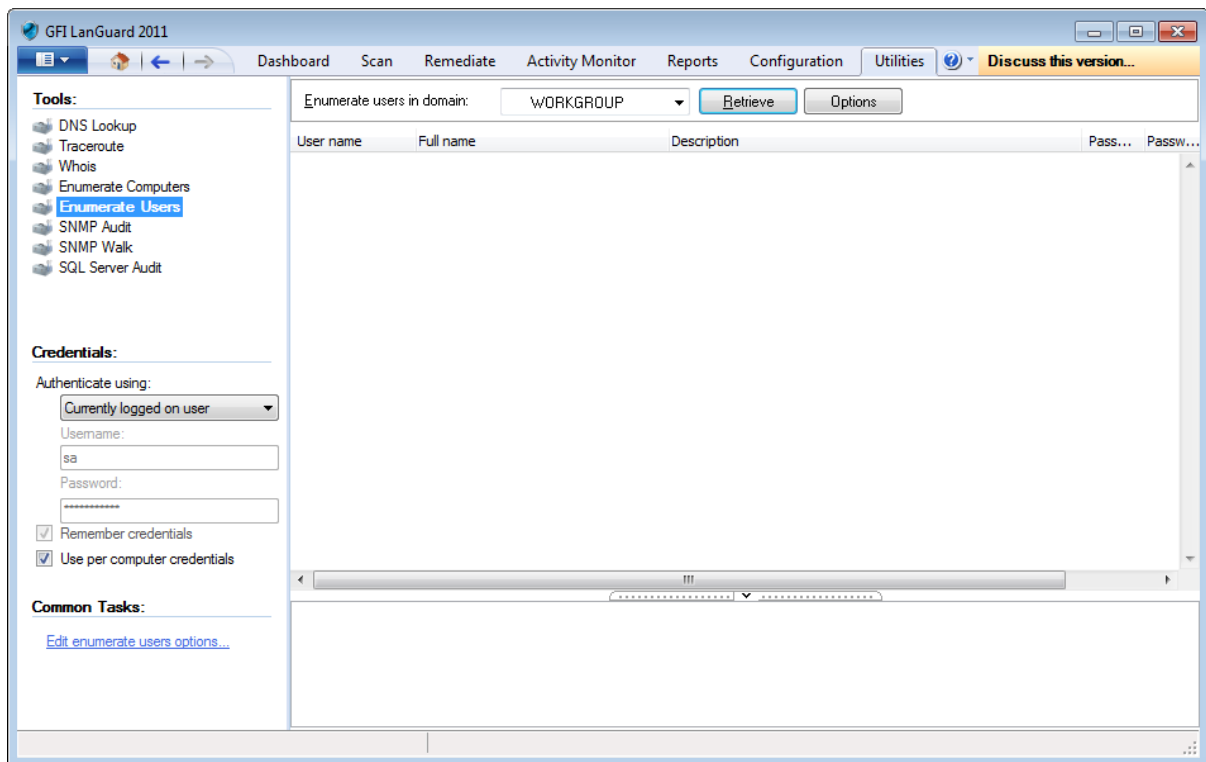
1. Select the computers that require deployment.
2. Right-click on any of the selected computers and select **Deploy Custom Patches**.

9.5.3 Enabling auditing policies

The **Enumerate Computers** tool also allows you to configure auditing policies on particular computers. This is done as follows:

1. Select the computers on which you want to enable auditing policies.
2. Right-click on any of the selected computers and select **Enable Auditing Policies...** This will launch the **Auditing Policies configuration Wizard** that will guide you through the configuration process.

9.6 Enumerate users



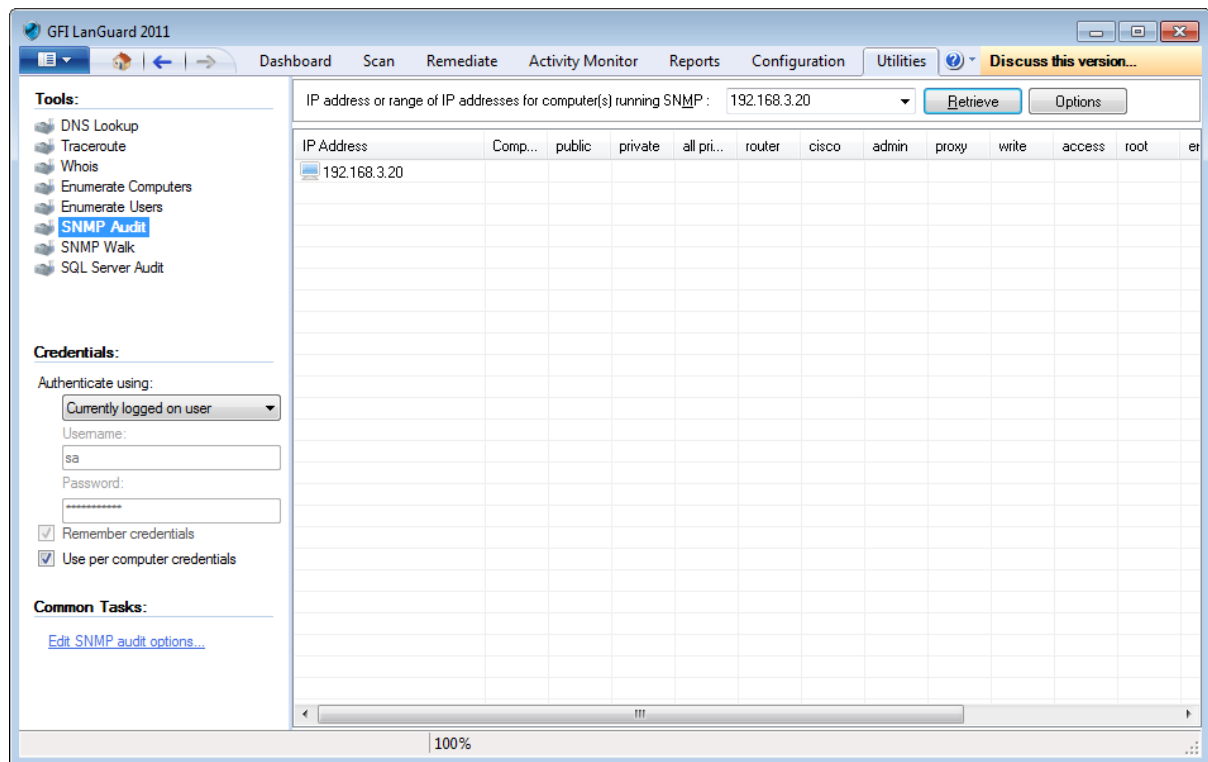
Screenshot 141 - The Enumerate Users tool dialog

To scan the Active Directory and retrieve the list of all users and contacts included in this database:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **Enumerate Users** in the left pane under **Tools**.
3. In the **Enumerate users in domain** dropdown menu, select the desired domain.
4. From **Common Tasks** in the left pane, click **Edit Enumerate Users options...** or **Options** on the right pane to filter the information to extract and display only the users or contacts details. In addition, you can optionally configure this tool to highlight disabled or locked accounts.
5. Click **Retrieve** to start the process.

This tool can enable or disable enumerated user accounts. Right-click on the account and select **Enable/Disable account** accordingly.

9.7 SNMP Auditing



Screenshot 142 - SNMP Audit tool

This tool identifies and reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary file (snmp-pass.txt).

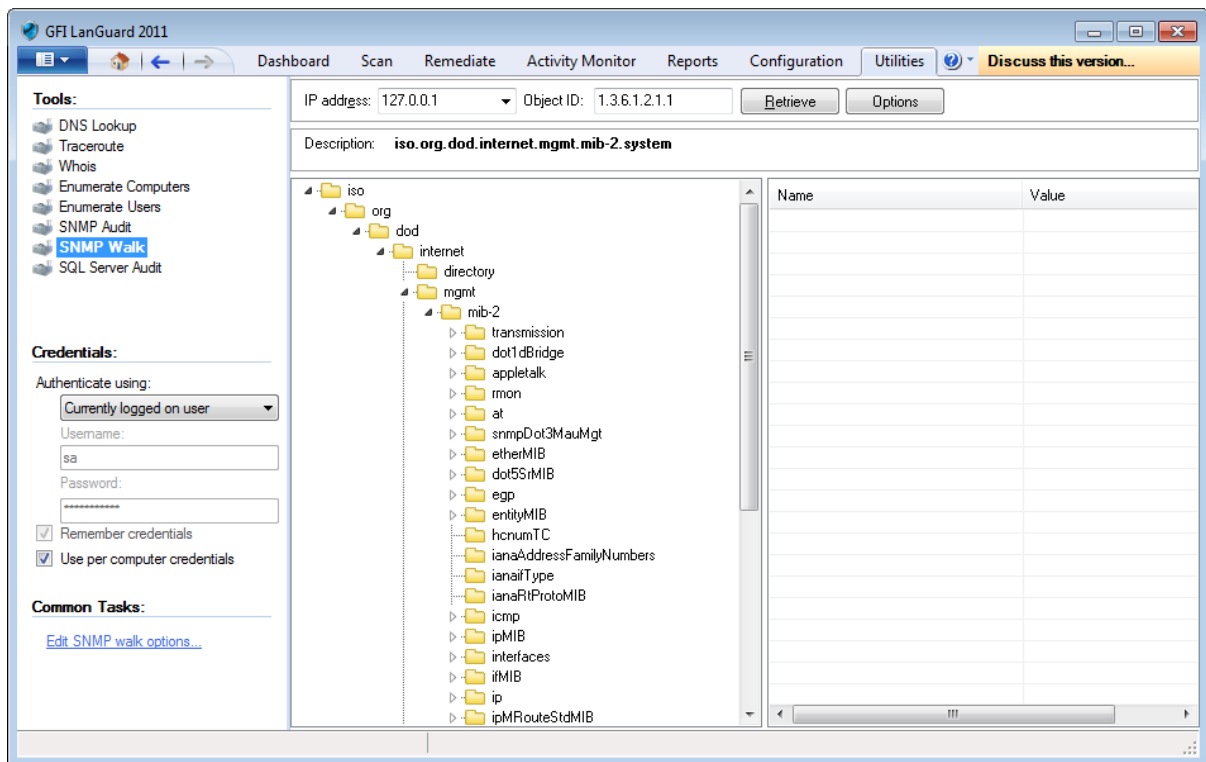
You can add new community strings to the default dictionary file by using a text editor (for example, notepad.exe).

You can also direct the **SNMP Audit** tool to use other dictionary files. To achieve this, specify the path to the dictionary file that you want to from the tool options at the right of the management console.

To perform SNMP audits on network targets and identify weak community strings:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **SNMP Audit** in the left pane under **Tools**.
3. In the **IP of computer running SNMP** dropdown, specify the IP to reach.
4. From **Common Tasks** in the left pane, click on **Edit SNMP Audit options...** or **Options** on the right pane to edit the default options.
5. Click **Retrieve** to start the process.

9.8 SNMP Walk



Screenshot 143 - SNMP Walk

To probe your network nodes and retrieve SNMP information (for example, OID's):

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **SNMP Walk** in the left pane under **Tools**.
3. In the **IP address** dropdown menu, specify the IP address of the computer that you wish to scan for SNMP information.
4. From **Common Tasks** in the left pane, click **Edit SNMP Walk options...** or **Options** on the right pane to edit the default options such as providing alternative community strings.
5. Click **Retrieve** to start the process.



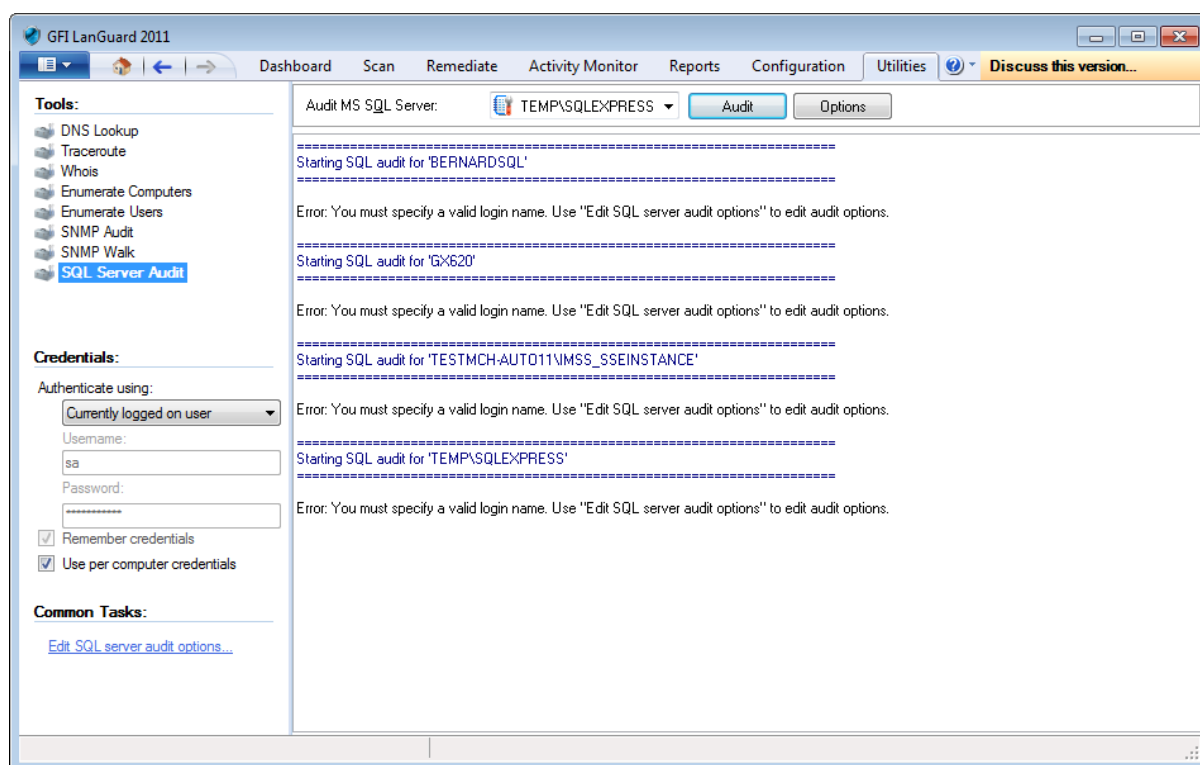
SNMP activity is normally blocked at the router / firewall so that internet users cannot SNMP scan your network. Malicious users can use information enumerated through SNMP scanning to hack your network / systems. Unless this service is required, it is highly recommended to disable it.

9.9 SQL Server Audit

This tool allows you to test the password vulnerability of the 'sa' account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server. During the audit process, this tool will perform dictionary attacks on the SQL server accounts using the credentials specified in the 'passwords.txt' dictionary file. However, you can also direct the **SQL Server Audit** tool to use other dictionary files. You can also customize your dictionary file by adding new passwords to the default list.

To perform a security audit on a particular Microsoft SQL server installation:

1. Launch GFI LanGuard management console from **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011**.
2. Click **Utilities** tab and select **SQL Server Audit** in the left pane under **Tools**.



Screenshot 144 -SQL Server Audit

3. In the **Audit MS SQL Server** dropdown menu, specify the IP address of the SQL Server that you wish to audit.
4. From **Common Tasks** in the left pane, click **Edit SQL Server Audit options...** or **Options** button on the right pane to edit the default options such as performing dictionary attacks on all the other SQL user accounts.
5. Click **Audit** to start the process.

10 Using GFI LanGuard from the command line

10.1 Introduction

In this chapter you will discover how to use the three command line tools bundled with GFI LanGuard; 'Insscmd.exe', 'deploycmd.exe' and 'impex.exe'. These command line tools allow you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up the GFI LanGuard management console.

Configured through a set of command line switches, the complete list of supported switches together with a description of the respective function is provided below.

10.2 Using the command line scanning tool: Insscmd.exe

The 'Insscmd.exe' command line target-scanning tool allows you to run vulnerability checks against network targets directly from the command line, or through third party applications, batch files and scripts. The 'Insscmd.exe' command line tool supports the following switches:

```
Insscmd [Target] [/profile=profileName] [/report=reportPath] [/output=pathToXmlFile]
[/user=username /password=password] [/UseComputerProfiles] [/email=emailAddress]
[/DontShowStatus] [/?]
```

Table 51 - Insscmd command switches

SWITCH	DESCRIPTION
Target	Specify the IP / range of IPs or host name(s) to be scanned.
/Profile	(Optional) Specify the scanning profile that will be used during a security scan. If this parameter is not specified, the scanning profile that is currently active in the GFI LanGuard will be used. NOTE: In the management console, the default (i.e. currently active) scanning profile is denoted by the word (Active) next to its name. To view which profile is active expand the Configuration tab ► Scanning Profiles node.
/Output	(Optional) Specify the full path (including filename) of the XML file where the scan results will be saved.
/Report	(Optional) Specify the full path (including filename) of the HTML file where the scan results HTML report will be output/saved.
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during security scanning. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the dashboard. For more information on how to configure computer credentials using the dashboard, refer to Configure credentials section in this manual.
/Email	(Optional) Specify the email address on which the resulting report(s) will be sent at the end of this scan. Reports will be emailed to destination through the mail server currently configured in the Configuration tab ► Alerting Options node (of the management console).
/DontShowStatus	(Optional) Include this switch if you want to perform silent scanning. In this way, the scan progress details will not be shown.
/?	(Optional) Use this switch to show the command line tool usage instructions.



Always enclose full paths and profile names within double quotes. For example, "[path or path name]" or "C:\temp\test.xml".

The command line target-scanning tool allows you to pass parameters through specific variables. These variables will be automatically replaced with their respective value during execution. Table 52 below describes the supported variables:

Table 52 - Supported variables in insscmd

SUPPORTED VARIABLE	DESCRIPTION
%INSTALLDIR%	During scanning, this variable will be replaced with the path to the GFI LanGuard installation directory.
%TARGET%	During scanning this variable will be replaced with the name of the target computer.
%SCANDATE%	During scanning this variable will be replaced with the date of scan.
%SCANTIME%	During scanning this variable will be replaced with the time of scan.

For example, how to launch target computer scanning from the command line tool. For this example, we will be assuming that a scan with the following parameters is required:

1. Perform a security scan on a target computer having IP address '130.16.130.1'.
2. Output the scan results to 'c:\out.xml' (i.e. XML file).
3. Generate an HTML report and save it in 'c:\result.html'.
4. Send the HTML report via email to 'lanss@127.0.0.1'

The command line tool instruction for this particular security scan is:

```
insscmd.exe 130.16.130.1 /Profile="Default" /Output="c:\out.xml" /Report="c:\result.html" /email="lanss@127.0.0.1"
```

10.3 Using the command line patch deployment tool: deploycmd.exe

The 'deploycmd.exe' command line patch deployment tool allows you to deploy Microsoft patches and third party software on remote targets directly from the command line, or through third party applications, batch files or scripts. The 'deploycmd.exe' command line tool supports the following switches:

```
deploycmd [target] [/file=FileName] [/username=UserName /password=Password]
[/UseComputerProfiles] [/warnuser] [/userapproval] [/stopservices]
[/customshare=CustomShareName] [/reboot] [/rebootuserdecides] [/shutdown]
[/deletefiles] [/timeout=Timeout(sec)] [/?]
```

Table 53 - deploycmd command switches

SWITCH	DESCRIPTION
Target	Specify the name(s), IP or range of IPs of the target computer(s) on which the patch(es) will be deployed.
/File	Specify the file that you wish to deploy on the specified target(s).
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during patch deployment. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the Dashboard. For more information on how to configure computer credentials using the dashboard, refer to Configure credentials section in this manual.
/warnuser	(Optional) Include this switch if you want to inform the target computer user that a file/patch installation is in progress. Users will be informed through a message dialog that will be shown on screen immediately before the deployment session is started.

SWITCH	DESCRIPTION
/userapproval	(Optional) Include this switch to request the user's approval before starting the file/patch installation process. This allows users to postpone the file/patch installation process for later (for example, until an already running process is completed on the target computer).
/stopservice	(Optional) Include this switch if you want to stop specific services on the target computer before installing the file/patch. NOTE: You cannot specify the services that will be stopped directly from the command line tool. Services can only be added or removed through the management console.
/customshare	(Optional) Specify the target share where you wish to transfer the file before it is installed.
/reboot	(Optional Parameter) Include this switch if you want to reboot the target computer after file/patch deployment.
/rebootuserdecides	(Optional Parameter) Include this switch to allow the current target computer user to decide when to reboot his computer (after patch installation).
/shutdown	(Optional Parameter) Include this switch if you want to shutdown the target computer after the file/patch is installed.
/deletefiles	(Optional Parameter) Include this switch if you want to delete the source file after it has been successfully installed.
/timeout	(Optional Parameter) Specify the deployment operation timeout. This value defines the time that a deployment process will be allowed to run before the file/patch installation is interrupted.
/?	(Optional) Use this switch to show the command line tool's usage instructions.

For example, how to launch a patch deployment process from the command line tool.

For this example, we will be assuming that a patch deployment session with the following parameters is required:

1. Deploy a file called '**patchA001002.XXX**'.
2. On target computer '**TMJohnDoe**'.
3. Reboot the target computer after successful deployment of the file.

The command line tool instruction for this particular patch deployment session is:

`deploycmd TMJohnDoe /file="patchA001002.XXX" /reboot`

10.4 Using the command line import and export tool: **impex.exe**

The Impex tool is a command line tool that can be used to Import and Export profiles and vulnerabilities from GFI LanGuard Network Security Scanner. The parameters supported by this tool are the following:

```
impex [[/H] | [/?]] | [/XML:xmlfile [/DB:dbfile] [/EX] [/MERGE]] | [/IM [/ONLYNEWER]]
[/PROFILES | /VULNS | /PORTS | /PROFILE:name | /VULNCAT:cat [/VULN:name]
/PORTTYPE:type [/PORT:number]] [/SKIP | /OVERWRITE | /RENAME:value]]
```

Table 54 - *impex* command switches

OPTION	DESCRIPTION
H, /?, running without parameters	Displays help information.
/XML:<xmlfile>	This parameter specifies the name of the imported or exported XML file. <xmlfile> needs to be replaced with the name of the file the profile is being exported to. NOTE: This parameter is mandatory to import or export alerts.

OPTION	DESCRIPTION
/DB:<dbfile>	Where <dbfile> is the database file to be used during the import/export operation. If this is not specified the default "operationsprofiles.mdb" file will be used.
/EX	Exports data from database to XML file (Default option)
/MERGE	If this is specified when the target XML for export already exists, the file will be opened and data will be merged; otherwise the XML file is first deleted.
/IM	Imports data from XML file to database
/ONLYNEWER	When specified only vulnerabilities newer than the newest vulnerability in the database will be imported.
/PROFILES	Exports/Imports all scanning profiles.
/VULNS	Exports/Imports all vulnerabilities.
/PORTS	Exports/Imports all ports
/PROFILE:<name>	Exports/Imports the specified scanning profile.
/VULNCAT:<category>	Exports/Imports all vulnerabilities of the specified category.
/VULN:<name>	Exports/Imports the specified vulnerability (/VULNCAT must be specified).
/PORTTYPE:<type>	Exports/Imports all ports of the specified type.
/PORT:<number>	Exports/Imports the specified port (/PORTTYPE must be specified).
/SKIP	If an item already exists in the target XML/database, that item will be skipped
/OVERWRITE	If an item already exists in the target XML/database, that item will be overwritten.
/RENAME:<value>	If an item already exists in the target XML/database, that item will be renamed to <value>. If /PROFILE or /VULN was specified, port information merged with that item is a port or renamed by prefixing its name with <value> in any other case.

Example, to export a specific alert:

» impex /xml:regcheck.xml /vuln:"Blaster Worm" /vulncat:"Registry Vulnerabilities"

Example: To import a whole XML file:

» impex /xml:regcheck.xml /im



The Impex executable can be located in the GFI LanGuard installation folder.



If the specified <xmlfile>, <dbfile>, <name>, <category> or <value> contain any space character, the whole value must be placed between double quotes.



It is highly recommended not to use the Impex tool if GFI LanGuard application (LanGuard.exe) or LanGuard scanning profiles (scanprofiles.exe) are running.

For example, /VULN:"Apache: Apache doc directory"



It is recommended that if the vulnerabilities are imported into another installation; that installation will have the same build number as the one the database has been exported from.

11 Adding vulnerability checks

11.1 Introduction

Scripts that identify custom vulnerabilities can be created using any VBScript compatible scripting language. By default, GFI LanGuard ships with a script editor that you can use to create your custom scripts.

New checks must be included in the list of checks supported by GFI LanGuard. Use the **Vulnerability Assessment** tab to add new checks to the default list of vulnerability checks on a scan profile by scan profile basis.

GFI LanGuard also supports Python scripting. For more information on GFI LanGuard Python scripting, refer to this section in this manual.



Only expert users should create new vulnerability checks. Scripting errors and wrong configurations in a vulnerability check can result in false positives or provide no vulnerability information at all.

11.2 GFI LanGuard VBscript language

GFI LanGuard supports and runs scripts written in VBscript compatible languages. Use VBscript compatible languages to create custom scripts that can be run against your network targets.

Security auditing scripts can be developed using the script editor that ships with GFI LanGuard. This built-in script editor includes syntax highlighting capabilities as well as debugging features that support you during script development. Open the script editor from **Start ► Programs ► GFI LanGuard 2011 ► LanGuard Script Debugger**.



For more information on how to develop scripts using the built-in script editor, refer to the **Scripting documentation** help file included in **Start ► Programs ► GFI LanGuard 2011 ► LanGuard Scripting documentation**.



GFI does not support requests related to problems in custom scripts. You can post any queries that you may have about GFI LanGuard forums at <http://forums.gfi.com/>. Through this forum, you are able to share scripts, problems and ideas with other GFI LanGuard users.

11.2.1 Adding a vulnerability check that uses a custom VB (.vbs) script

To create new vulnerability checks that use custom VBscripts:

- » **Step 1: Create the script.**
- » **Step 2: Add the new vulnerability check.**

The following are examples of how this is done.

Step 1: Create the script

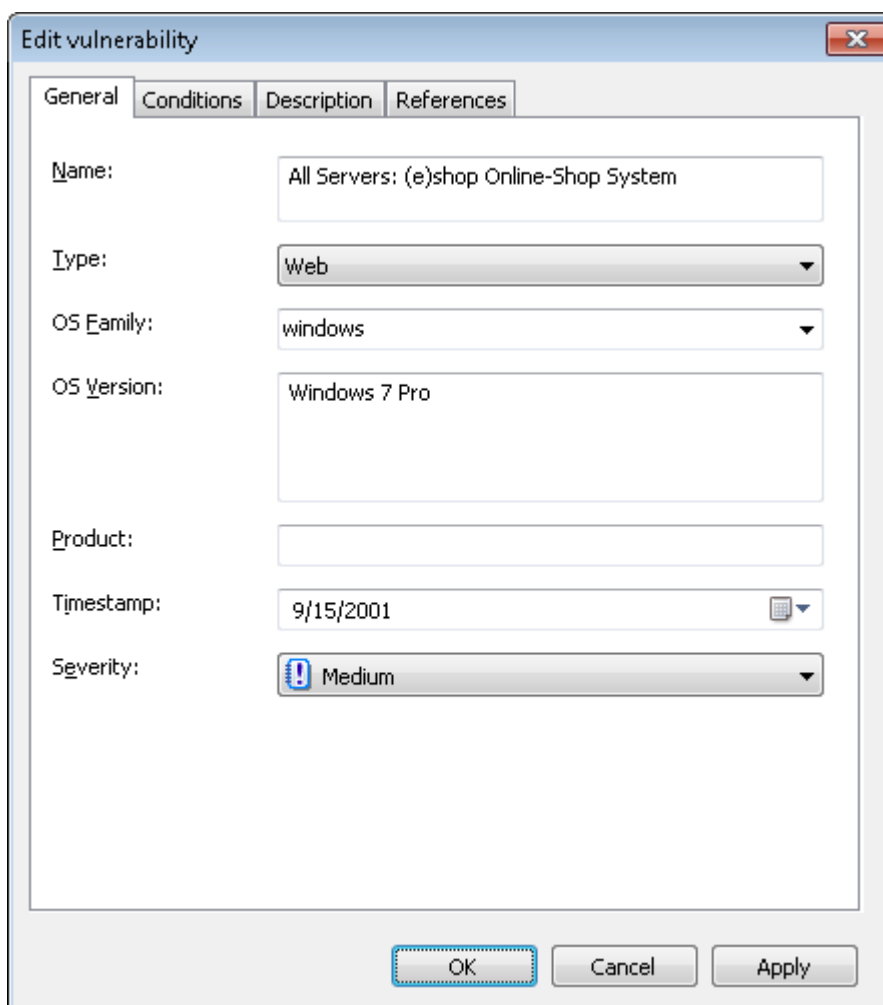
1. Launch the Script Debugger from **Start ► Programs ► GFI LanGuard 2011 ► LanGuard Script Debugger**.
2. Go on **File ► New...**
3. Create a script. For this example, use the following sample script code.

```
Function Main
    echo "Script has run successfully"
    Main = true
End Function
```

4. Save the script in '<LanGuard installation folder path> \Data\Scripts\myscript.vbs'.

Step 2: Add the new vulnerability check

1. Open the GFI LanGuard management console.
2. Click **Configuration** tab, and select **Scanning Profiles**.
3. Click **Vulnerability Assessment** sub-node and from the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities).



Edit vulnerability

General | Conditions | Description | References

Name: All Servers: (e)shop Online-Shop System

Type: Web

OS Family: windows

OS Version: Windows 7 Pro

Product:

Timestamp: 9/15/2001

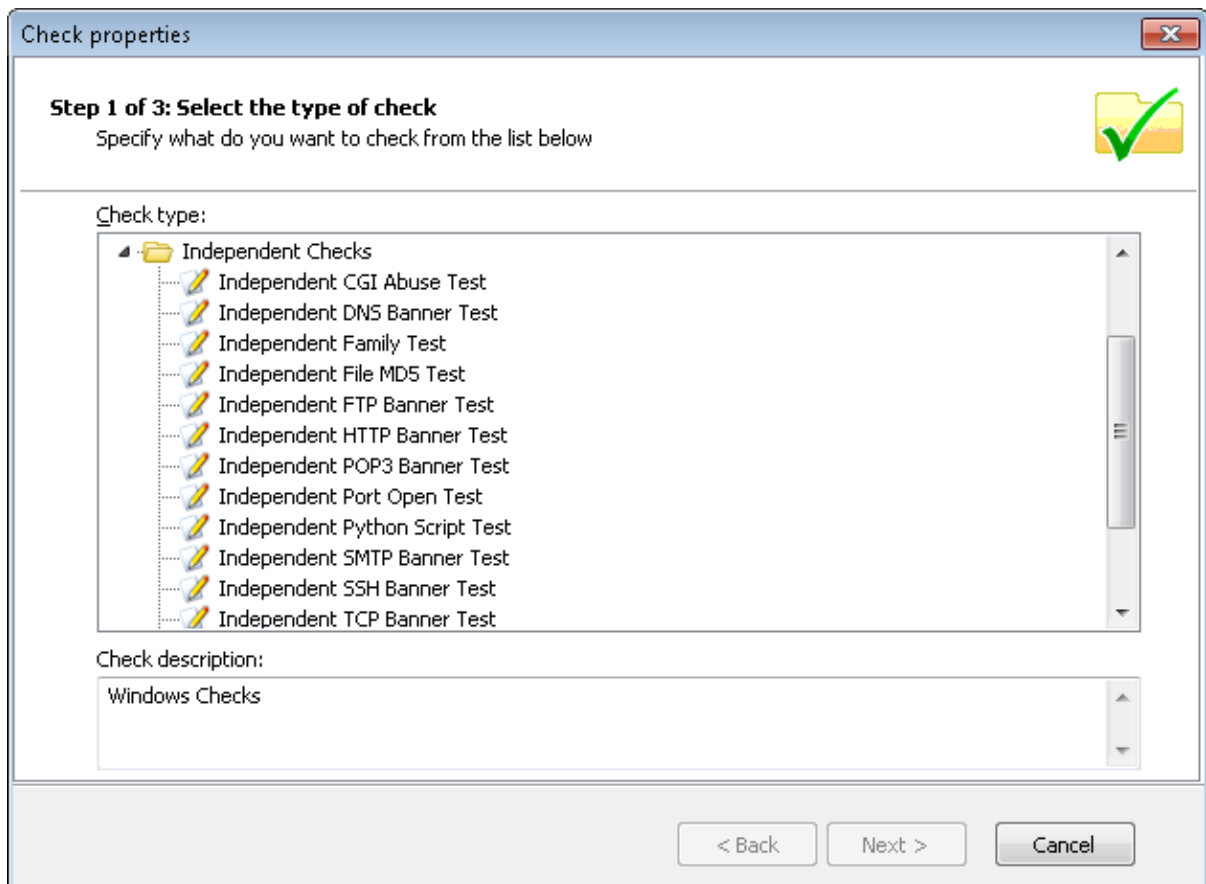
Severity: Medium

OK Cancel Apply

Screenshot 145 - The new vulnerability check dialog

4. In the new window, add a new vulnerability by clicking **Add...** in the middle pane.

5. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).
6. Click the **Conditions** tab and click on the **Add...** button. This will bring up the check properties wizard.



Screenshot 146 - The check triggering conditions dialog

7. Select **Independent checks** ► **VBScript** node and click **Next** button to continue setup.
8. Click **Choose file**  and select the custom VBScript file that will be executed by this check (For this example select 'myscript.vbs'). Click **Next** to proceed.
9. Select the relative condition setup in the wizard to finalize script selection. Click **Finish** to exit wizard.
10. Click **OK** to save new vulnerability check.

Testing the vulnerability check/script used in example

Scan your local host computer using the scanning profile where the new check was added.

In **Scan** tab ► **Results**, a vulnerability warning will be shown in the **Vulnerability Assessment** node of the scan results.

11.3 GFI LanGuard SSH Module

GFI LanGuard includes an SSH module which handles the execution of vulnerability scripts on Linux/UNIX based systems.

The SSH module determines the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX

vulnerability checks using any scripting method that is supported by the target operating system.

11.3.1 Keywords

The SSH module can run security scanning scripts through its terminal window. When a security scan is launched on Linux/UNIX based target computers, vulnerability checking scripts are copied through an SSH connection to the respective target computer and run locally.

The SSH connection is established using the logon credentials (i.e. username and password/SSH Private Key file) specified prior to the start of a security scan.

The SSH module can determine the status of a vulnerability check through specific keywords present in the text output of the executed script. These keywords are processed by the module and interpreted as instruction for the GFI LanGuard. Standard keywords identified by the SSH module include:

- » **TRUE:**
- » **FALSE:**
- » **AddListItem**
- » **SetDescription**
- » **!!SCRIPT_FINISHED!!**

Each of these keywords triggers an associated and specific process in the SSH Module. The function of each keyword is described below:

- » **TRUE: / FALSE:** - These strings indicate the result of the executed vulnerability check/script. When the SSH module detects a TRUE: it means that the check was successful; FALSE: indicates that the vulnerability check has failed.
- » **AddListItem** - This string triggers an internal function that adds results to the vulnerability check report (i.e. scan results). These results are shown in the GFI LanGuard 2011 management console after completion of a scan. This string is formatted as follows:
 - » **AddListItem([[[[parent node]]]],[[[actual string]]]])**
 - » **[[[parent node]]]** - Includes the name of the scan results node to which the result will be added.
 - » **[[[actual string]]]** - Includes the value that will be added to the scan results node.



Each vulnerability check is bound to an associated scan result node. This means that 'AddListItem' results are by default included under an associated/default vulnerability node. In this way, if the parent node parameter is left empty, the function will add the specified string to the default node.

- » **SetDescription** - This string triggers an internal function that will overwrite the default description of a vulnerability check with a new description. This string is formatted as follows: **SetDescription([New description])**
- » **!!SCRIPT_FINISHED!!** - This string marks the end of every script execution. The SSH module will keep looking for this string until it is found or until a timeout occurs. If a timeout occurs before the '!!SCRIPT_FINISHED!!' string is generated, the SSH module will classify the respective vulnerability check as failed.



It is imperative that every custom script outputs the '!!SCRIPT_FINISHED!!' string at the very end of its checking process

11.3.2 Adding a vulnerability check that uses a custom shell script

In the following example we will create a vulnerability check (for Linux based targets) which uses a script written in Bash. The vulnerability check in this example will test for the presence of a dummy file called 'test.file'

Step 1 : Create the script

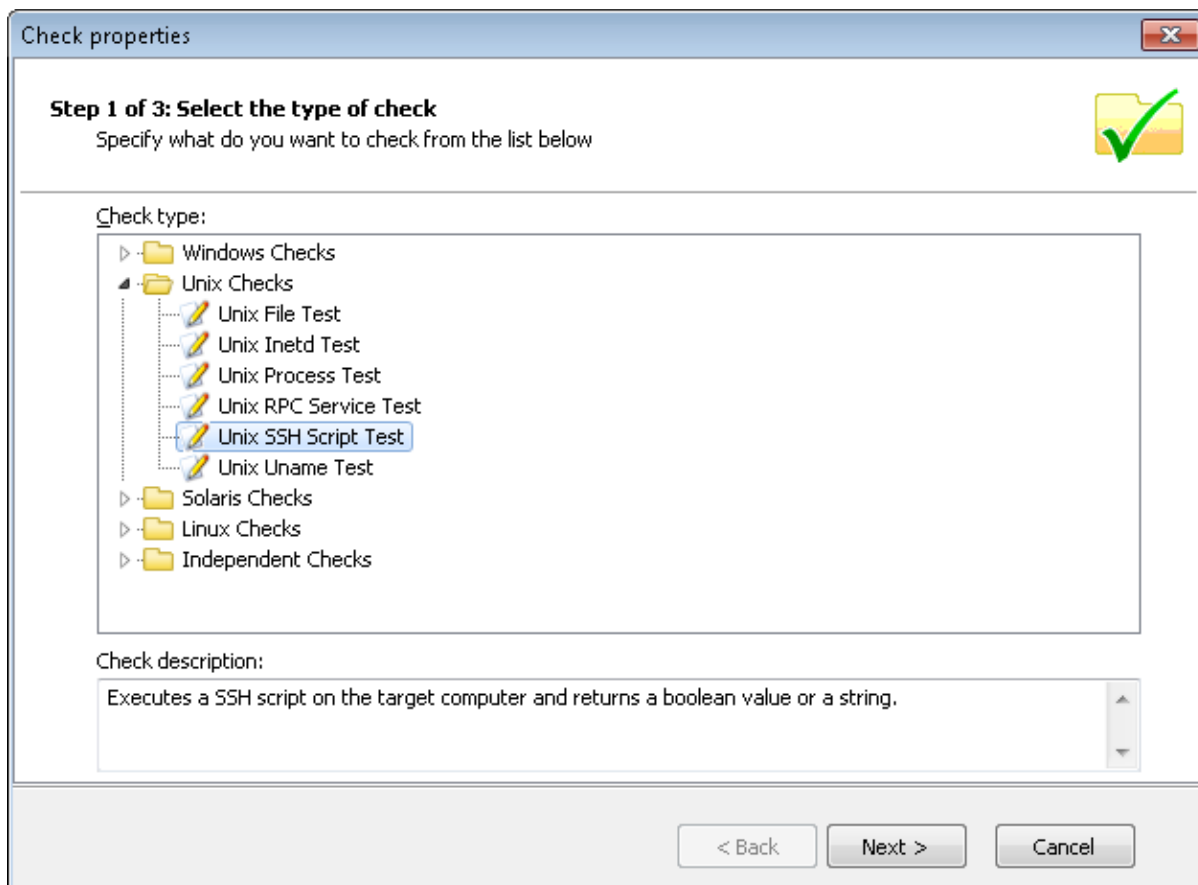
1. Launch your favorite text file editor.
2. Create a new script using the following code:

```
#!/bin/bash
if [ -e test.file ]
then
    echo "TRUE:"
else
    echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
```

3. Save the file in <GFI LanGuard 2011 installation folder path> ..\Data\Scripts\myscript.sh

Step 2: Add the new vulnerability check

1. Open the GFI LanGuard 2011 management console.
2. Click **Configuration** tab, expand the **Scanning Profiles** and click **Vulnerability Assessment** sub-node.
3. From the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities...).
4. In the new window, add a new vulnerability by clicking **Add...** in the middle pane.
5. Go through the General, Description and Reference tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).
6. Choose the **Conditions** tab and click **Add...** button. This will bring up the check properties wizard.



Screenshot 147 - The check triggering conditions dialog

7. Select **Unix checks** ► **SSH Script Test** node and click on Next button to continue setup.
8. Click **Choose file**  and select the custom SSH Script file that will execute during this check (For this example select 'myscript.sh'). Click **Next** to proceed.
9. Select the relative condition setup in the wizard to finalize script selection. Click **Finish** to exit wizard.
10. Click **OK** to save new vulnerability check.

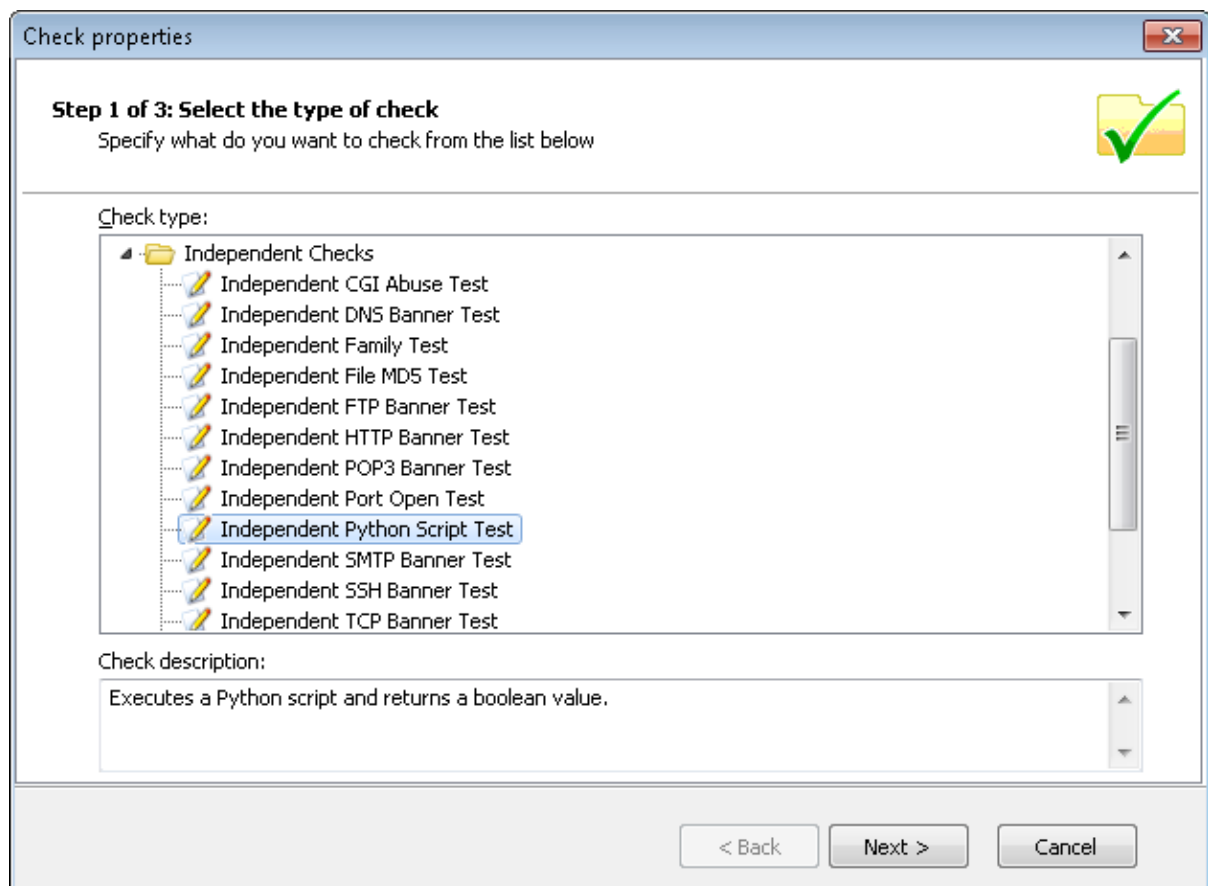
Testing the vulnerability check/script used in our example

Scan your local host computer using the scanning profile where the new check was added.

1. Log on to a Linux target computer and create a file called '**test.file**'. This check will generate a vulnerability alert if a file called '**test.file**' is found.
2. Launch a scan on the Linux target where you created the file.
3. Check you scan results.

11.4 Python scripting

GFI LanGuard also supports a new type of vulnerability checks - Python Script Test. This type of check is available under the Independent Checks type.



Screenshot 148 - Independent checks: Python Script Test

For more information on Python scripting refer to the GFI LanGuard scripting documentation located in **Start menu ► Programs ► GFI LanGuard 2011**.

12 GFI LanGuard certifications

12.1 Introduction

GFI LanGuard is OVAL and CVE certified.

12.2 About OVAL

Open Vulnerability and Assessment Language (OVAL™) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the OVAL community. The language standardizes the three main steps of the assessment process:

- » Representing configuration information of systems for testing
- » Analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.)
- » Reporting the results of this assessment.
- » The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three XML schemas to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process:

- » An OVAL System Characteristics schema for representing system information
- » An OVAL Definition schema for expressing a specific machine state
- » An OVAL Results schema for reporting the results of an assessment

Content written in OVAL Language is located in one of the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that the OVAL, which is funded by US-CERT at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

12.2.1 GFI LanGuard OVAL Support

GFI LanGuard supports all checks defined in the XML file issued by OVAL, with the exception of HP-UX checks.

GFI LanGuard does not support HP-UX based machines and therefore it is beyond the scope of this product to include these checks within its check definition database.

12.2.2 About OVAL Compatibility

OVAL Compatibility is a program established to develop consistency within the security community regarding the use and implementation of OVAL. The main goal of the compatibility program is to create a set of guidelines that will help enforce a standard implementation. An offshoot of this is that users are able to distinguish between, and have confidence in, compatible products knowing that the implementation of OVAL coincides with the standard set forth.

For a product or service to gain official OVAL Compatibility, it must adhere to the **Requirements and Recommendations for OVAL Compatibility** and complete the formal OVAL Compatibility Process.

OVAL Compatibility means that GFI LanGuard incorporates OVAL in a pre-defined, standard way and uses OVAL for communicating details of vulnerabilities, patches, security configuration settings, and other machine states.

12.2.3 Submitting OVAL listing error reports

Any issues with the GFI LanGuard or the listing of the OVAL checks included with GFI LanGuard should be reported to GFI through its official support lines. Refer to the [Troubleshooting](#) section within this manual for more information regarding email, phone or web forum support channels.

GFI Software Ltd will endeavor to look into any issues reported and if any inconsistency or error is ascertained, it will issue updates to fix such issues. Vulnerability check updates are usually released on monthly basis.

12.3 About CVE

CVE (Common Vulnerabilities and Exposures) is a list of standardized names for vulnerabilities and other information security exposures. Its aim is to standardize the names for all publicly known vulnerabilities and security exposures.

CVE is a dictionary which aim is to facilitate data distribution across separate vulnerability databases and security tools. CVE makes searching for information in other databases easier and should not be considered as a vulnerability database by itself.

CVE is maintained through a community-wide collaborative effort known as the CVE Editorial Board. The Editorial Board includes representatives from numerous security-related organizations such as security tool vendors, academic institutions, and governments as well as other prominent security experts. The MITRE Corporation maintains CVE and moderates editorial board discussions.

12.3.1 About CVE Compatibility

"CVE-compatible" means that a tool, Web site, database, or service uses CVE names in a way that allows it to cross-link with other repositories that use CVE names. CVE-compatible products and services must meet the four requirements:

CVE Searchable: A user must be able to search for vulnerabilities and related information using the CVE name.

CVE Output: Information provided must include the related CVE name(s).

Mapping: The repository owner must provide a mapping relative to a specific version of CVE, and must make a good faith effort to ensure accuracy of that mapping.

Documentation: The organization's standard documentation must include a description of CVE, CVE compatibility, and the details of how its customers can use the CVE-related functionality of its product or service.



For an in-depth understanding of CVE compatibility refer to the complete list of CVE requirements available at:
<http://cve.mitre.org/compatible/requirements.html>

12.3.2 About CVE and CAN

CVE names (also called "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. CVE names have "entry" or "candidate" status. Entry status indicates that the CVE name has been accepted to the CVE List while candidate status (also called "candidates," "candidate numbers," or "CANs") indicates that the name is under review for inclusion in the list.

Each CVE name includes the following:

- » CVE identifier number (i.e. "CVE-1999-0067").
- » Indication of "entry" or "candidate" status.
- » Brief description of the security vulnerability or exposure.
- » Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

For an in-depth understanding of CVE names and CANs, refer to:

<http://cve.mitre.org/cve/identifiers/index.html>

12.3.3 Searching for CVE entries in GFI LanGuard

CVE entries can be searched from the Scanning profiles node within the **Configuration** tab.

Find bulletin:

Search by bulletin name (e.g. MS02-017) or QNumber (e.g. Q311967).

Find Find next

Screenshot 149 - Searching for CVE information

To search for a particular CVE bulletin:

1. Specify the bulletin name (for example, CVE-2005-2126) in the search tool entry box included at the bottom of the right pane.
2. Click on **Find** to start searching for your entry.

12.3.4 Obtaining CVE names

CVE entry names can be obtained through the GFI LanGuard user interface from within the Scanning profiles node within the **Configuration** tab. By default, the CVE ID is displayed for all the vulnerabilities that have a CVE ID.

12.3.5 Importing and exporting CVE Data

CVE data can be exported through the impex command line tool. For more information on the impex command line tool refer to the [Using 'impex.exe' - the command line import and export tool](#) section within this manual

13 Miscellaneous

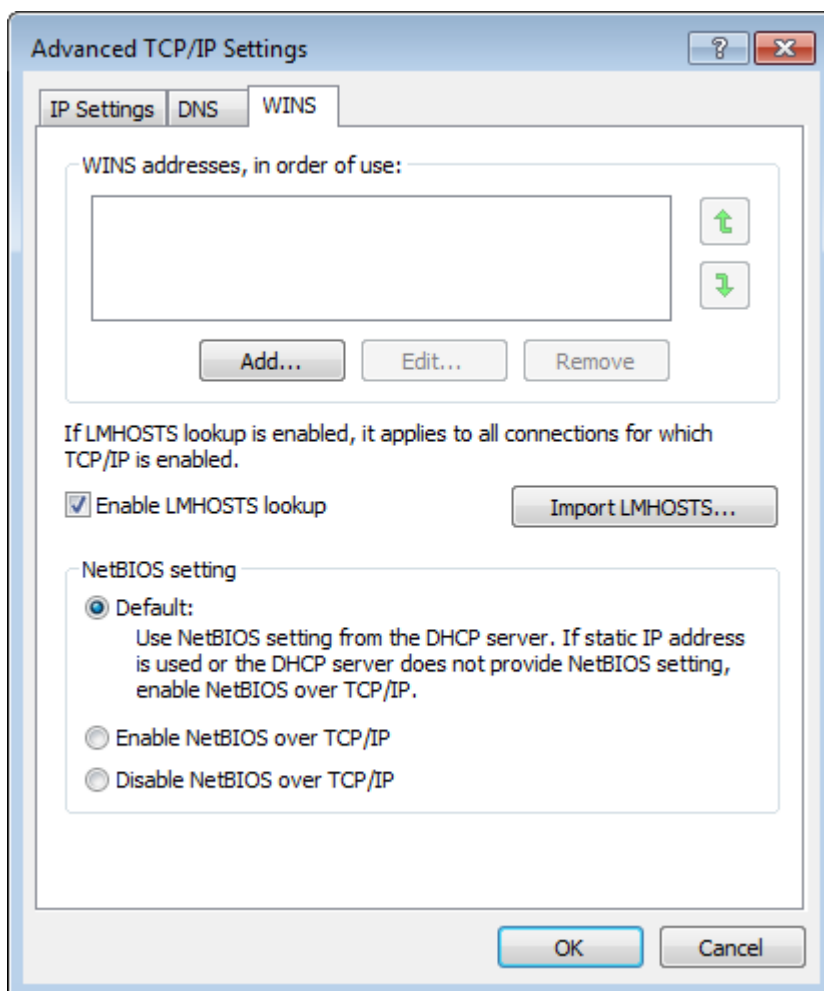
13.1 Enabling NetBIOS on a network computer

1. In Microsoft Windows 7 and Microsoft Windows Vista, navigate to **Control Panel ► Network and Internet ► Network and Sharing Center ► Change adapter settings**.



In Microsoft Windows XP, click **Control Panel ► Network Connections**.

2. Right-click on **Local Area Connection** and select **Properties**.
3. Click **Internet Protocol (TCP/IP)** and select **Properties**.
4. Click **Advanced ► WINS**.



Screenshot 150 - Local Areas Connection properties: WINS tab

5. Select the **Default** option from the **NetBIOS Setting** area.
6. Click **OK** and exit the **Local Area Properties** dialog(s).



If static IP is being used or the DHCP server does not provide NetBIOS setting, select the **Enable NetBIOS over TCP/IP** option

14 Troubleshooting

14.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. It explains the use of the GFI LanGuard troubleshooting wizard. The main sources of information available to users are:

- » The manual - most issues can be solved by reading this manual.
- » The GFI Knowledge Base - <http://kbase.gfi.com>
- » The GFI technical support site - <http://support.gfi.com>
- » The GFI Web forum - <http://forums.gfi.com/>
- » Contacting the GFI technical support team by email at support@gfi.com
- » Contacting the GFI technical support team using our live support service at <http://support.gfi.com/livesupport.asp>
- » Contacting our technical support team by telephone.

14.2 Common Issues

Table 55 - GFI LanGuard common issues

ISSUE ENCOUNTERED	SOLUTION / DESCRIPTION
When trying to access the Change database tab while configuring an SQL database, a Failed to connect to database error is encountered.	Description: This issue may occur when the following two conditions are met: GFI LanGuard is installed on Windows 2000 SP4 with MDAC 2.5 SP 3. And The database backend is Microsoft SQL having the database instance name different from the SQL machine name. Solution: Install Microsoft Data Access Components (MDAC 2.6 or later) on the GFI LanGuard machine and try again. MDAC can be downloaded from: http://www.microsoft.com/downloads/details.aspx?FamilyID=6c050fe3-c795-4b7d-b037-185d0506396c&displaylang=en

ISSUE ENCOUNTERED	SOLUTION / DESCRIPTION
Incomplete results and errors when scanning remote machines.	Description: Errors similar to the following may be encountered: » Failed to open test key to remote registry. » The scan will not continue. » Access Denied. » Could not connect to remote SMB server. These errors may be encountered because: » The remote machine has an account similar to the one used by GFI LanGuard to log in as an administrator. » The user account used by GFI LanGuard does not have administrative privileges. Solution: To solve this issue do one of the following: » Log on the GFI LanGuard machine and configure GFI LanGuard to use an alternate domain administrator account. » Delete the local user account on the remote machine. » Launch GFI LanGuard executable with 'Run As' using a Domain Administrator account. For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003125.
GFI LanGuard program updates not working.	Description: Updates will not work if GFI LanGuard machine does not have a direct connection to the internet. Solution: To solve this issue do one of the following: » Configure GFI LanGuard machine to have direct internet access. » Install another instance of GFI LanGuard on a machine with internet access and configure GFI LanGuard to check for updates from the new installation. For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID002062
Firewall installed on GFI LanGuard is blocking connection with target computers.	Description: Scanning might slow down or blocked if a firewall is installed on GFI LanGuard machine. Solution: Configure the firewall to allow the following components in outbound connections: » <..\Program Files\GFI\LanGuard>\LanGuard.exe » <..\Program Files\GFI\LanGuard>\lnsscomm.exe » <..\Program Files\GFI\LanGuard>\lnssatt.exe » <..\Program Files\GFI\LanGuard>\update.exe
GFI LanGuard is failing to retrieve workgroup computers when using Enumerate Computers.	Description: GFI LanGuard uses the Windows mechanism to retrieve the machines within a workgroup. In this mechanism a Master Browser computer will create and store a list of all computers. In some cases, the Master Browser role can fail resulting in GFI LanGuard not retrieving computers information. To solve this issue, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003483

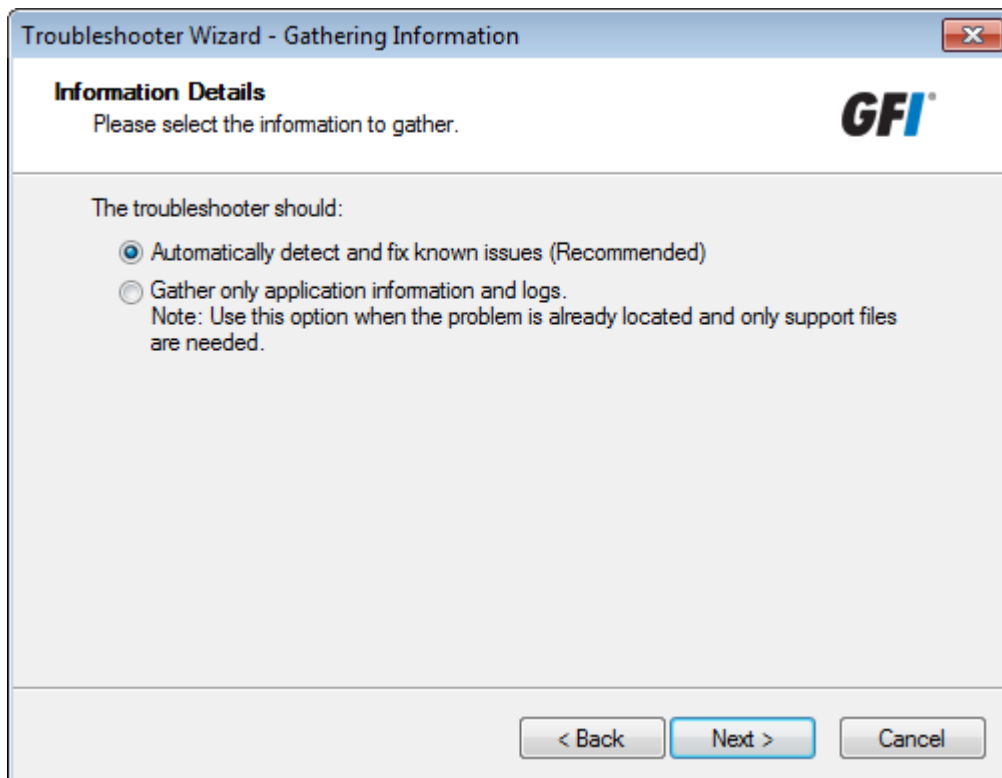
ISSUE ENCOUNTERED	SOLUTION / DESCRIPTION
GFI LanGuard found open ports that another port scanner found closed.	Description: GFI LanGuard uses a different approach than other port scanners to detect open ports. Solution: To view the status of a port and determine if the port is closed or opened: 1. Click Start ► Programs ► Accessories ► Command Prompt. 2. Key in netstat -an, and press Enter. 3. The generated list displays all computer active connections. For more information refer to: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netstat.msp?mfr=true.

14.3 The Troubleshooting wizard

The GFI LanGuard troubleshooting wizard is a tool designed to assist you when encountering technical issues related to GFI LanGuard's use.

To use the GFI LanGuard troubleshooting wizard:

1. Launch the troubleshooting wizard from the **Start ► Programs ► GFI LanGuard 2011 ► GFI LanGuard 2011 Troubleshooter**.
2. Click **Next** in the introduction page.



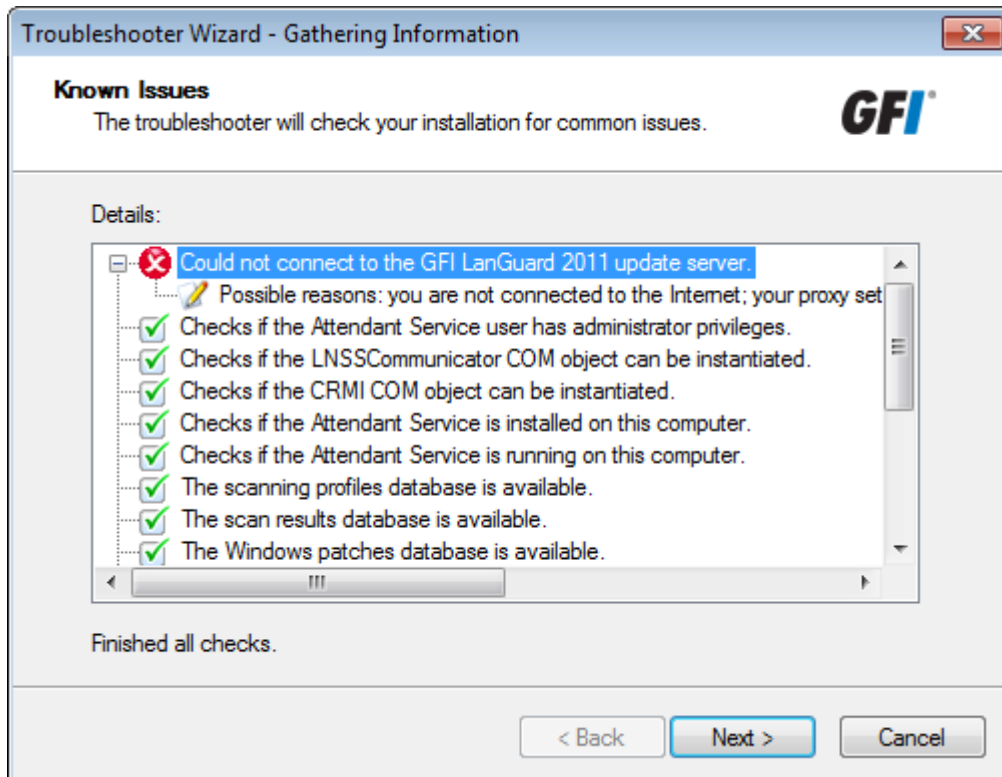
Screenshot 151 - Troubleshooter wizard - Information details

3. In the Information details page select one of the following options described below:

Table 56 - Information gathering options

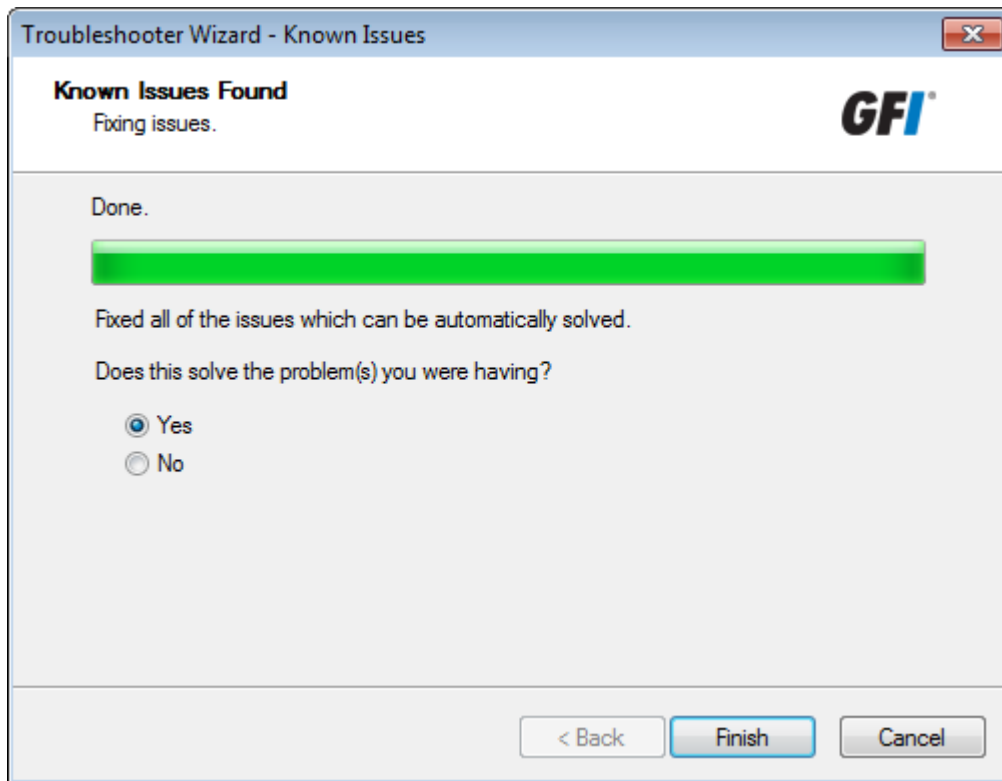
OPTION	DESCRIPTION
Automatically detect and fix known issues	(Recommended) Configure GFI LanGuard to automatically detect and fix issues.
Gather only application information and logs	Gather logs to send to GFI support.

4. Click **Next** to continue.



Screenshot 152 - Troubleshooter wizard - Gathering information about known issues

5. The troubleshooter wizard will retrieve all the information required to solve common issues. Click **Next** to continue.



Screenshot 153 - Troubleshooter fixed known issues

6. The troubleshooter will fix any known issues that it encounters. Select **Yes** if your problem was fixed or **No** if your problem is not solved to search the GFI Knowledge base for information.

14.4 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit <http://kbase.gfi.com/>.

14.5 Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

14.6 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

Online: Fill out the support request form on: <http://support.gfi.com/supportrequestform.asp>. Follow the instructions on the page to submit your support request.

Phone: To obtain the correct technical support phone number for your region visit: <http://www.gfi.com/company/contact.htm>. We will answer your query within 24 hours or less depending on your time zone.



Before you contact our Technical Support team ensure that you have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at <http://customers.gfi.com>.

14.7 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit:

<http://www.gfi.com/pages/productmailing.htm>

15 Glossary

TERM	DESCRIPTION
Active Directory	A technology that provides a variety of network services, including LDAP-like directory services.
AD	See Active Directory
Anti-spyware	A software countermeasure that detects spyware installed on a computer without the user's knowledge.
Anti-virus	A software countermeasure that detects malware installed on a computer without the user's knowledge.
Apache web server	An open source HTTP server project developed and maintained by the Apache software foundation.
Applications auto-uninstall	An action that enables the auto-uninstall of applications that support silent uninstall from GFI LanGuard.
Auto-download	A GFI LanGuard technology that automatically downloads missing patches and service packs in all 38 languages.
Auto-patch management	A GFI LanGuard technology that automatically downloads missing Microsoft updates and deploys them over the network.
Auto-remediation	A GFI LanGuard technology that automatically downloads and deploy missing patches. If an application is blacklisted in GFI LanGuard, auto-remediation will uninstall the application from the target computer during scheduled operations.
Backdoor program	An alternative method used to access a computer or computer data over a network.
Batch-files	A text files containing a collection of instructions to be carried out by an operating system or an application.
Blacklist	A list of USBs or Network devices names that are considered as dangerous. When a USB\Network device name contains a blacklisted entry while scanning a network, GFI LanGuard will report the device as a security threat (High security vulnerability).
Bluetooth	An open wireless communication and interfacing protocol that enables exchange of data between devices.
Bulletin Information	Contains a collection of information about a patch or a Microsoft update. Used in GFI LanGuard to provide more information on an installed patch or update. Information includes; Bulletin id, title, description, URL and file size.
CGI requests	See Common Gateway Interface
Common Gateway Interface	A communication script used by web servers to transfer data to a client internet browser.
Common Vulnerabilities and Exposures	A list of standardized names for vulnerabilities and other information security exposures. The aim of CVE is to standardize the names for all publicly known vulnerabilities and security exposures.
CVE	See Common Vulnerabilities and Exposures
Dashboard	A graphical representation that indicates the status of various operations that might be currently active, or that are scheduled.
Demilitarized Zone	A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.
deploycmd.exe	A GFI LanGuard command line tool, used to deploy Microsoft patches and third party software on target computers.
DMZ	See Demilitarized Zone
DNS	See Domain Name System
DNS Lookup tool	A utility that converts domain names into the corresponding IP address and retrieves particular information from the target domain
Domain Name System	A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

TERM	DESCRIPTION
Enumerate computers tool	A utility that identifies domains and workgroups on a network.
Enumerate users tools	A tools that enables the scanning of the Active Directory and the retrieval of the list of all users and contacts included in this database:
Extensible Markup Language	An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.
File Transfer Protocol	A protocol used to transfer files between computers
FTP	See File Transfer Protocol
GFI EndPointSecurity	A security solution developed by GFI that helps organizations to maintain data integrity by preventing unauthorized access and transfers from removable devices.
GFI LanGuard ReportPack	A reporting application developed by GFI to generate graphical reports based on results generated by GFI LanGuard.
GPO	See Group Policy Object
Group Policy Object	An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.
ICMP pings	See Internet Control Message Protocol
IDS	See Intrusion Detection Software
impex.exe	A Command line tool, used to Import and Export profiles and vulnerabilities from GFI LanGuard.
Internet Control Message Protocol	A protocol used by network devices to send network related errors.
Internet Information Services	A set of Internet-based services created by Microsoft Corporation for internet servers.
Linux	An open source operating system that is part of the Unix operating systems family.
Insscmd.exe	A GFI LanGuard command line tool that allows running vulnerability checks against network targets.
Local Host	In networking, the local host is the computer you are currently using. One can reference to the local host by using the reserved IP address 127.0.0.1 In this manual the Local host is the machine were GFI LanGuard is installed.
Mail server	The server that manages and stores client's emails
Malware	Composed from malicious and software, malware is a general term used for all software developed to harm and damage a computer system. Viruses, worms and Trojans are all type of malware.
Microsoft Access database	A Microsoft desktop relational database management system included in the Microsoft Office package. Microsoft Access is normally used for small databases.
Microsoft IIS	See Internet Information Services
Microsoft SQL Server	A Microsoft relational database management system. Microsoft included extra functionality to the SQL Server (transaction control, exception handling and security) so that Microsoft SQL server can support large organizations
Microsoft Windows service packs	A collection of updates and fixes provided by Microsoft to improve an application or an operating system.
Microsoft WSUS	An acronym for Microsoft Windows Server Update Services. This service enables administrators to manage the distribution of Microsoft updates to network computers.
MS-Access	See Microsoft Access database
MS-SQL	See Microsoft SQL Server
NETBIOS	An acronym for Network Basic Input/output. This system provides services to allow applications on different computers within a network to communicate with each other.
Netscape	A web browser originally developed by Netscape Communications Corporation.

TERM	DESCRIPTION
Open Vulnerability and Assessment Language	A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.
OVAL	See Open Vulnerability and Assessment Language
Patch agent	A background service that handles the deployment of patches, service packs and software updates on target computers.
Python scripting	A high-level computer programming scripting language.
Remote Desktop Protocol	A protocol developed by Microsoft to enable clients to connect with the user interface of a remote computer.
SANS	An acronym for System Administration, Networking and Security research organization. An institute that shares solutions regarding system and security alerts.
Scan profiles	A collection of vulnerability checks that determine what vulnerabilities are identified and which information will be retrieved from scanned targets.
Script Debugger	A GFI LanGuard module that allows you to write and debug custom scripts using a VBScript-compatible language.
SNMP	Acronym for Simple Network Management Protocol, a technology used to monitor network devices such as, routers, hubs and switches.
SNMP Auditing tool	A tool that reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary
SNMP Walk tool	A tool used to probe your network nodes and retrieve SNMP information
Spyware	A form of malware intended to collect information from a computer without notifying the user.
SQL Server Audit tool	A tool used to test the password vulnerability of the 'sa' account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server
SSH Module	A module used to determine the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target's Linux/UNIX OS and which outputs results to the console in text.
TCP ports	Acronym for Transmitting Control Protocol. This protocol is developed to allow applications to transmit and receive data over the internet using the well-known computer ports
Terminal Services	A service that allows connecting to a target computer and managing its installed applications and stored data.
Traceroute tool	A tool used to identify the path that GFI LanGuard followed to reach a target computer.
Trojans	A form of malware that contains a hidden application that will harm a computer.
UDP ports	An acronym for User Datagram Protocol, these used to transfer UDP data between devices. In this protocol received packets are not acknowledged.
Uniform Resource Locator	The Uniform Resource Locator is the address of a web page on the world wide web.
Universal Serial Bus	A Serial bus standard widely used to connect devices to a host computer
URL	See Uniform Resource Locator
USB	See Universal Serial Bus
VBScript	A Visual Basic Scripting language is a high-level programming language developed by Microsoft.
Virus	A form of malware that infects a computer. The aim of a virus is to harm a computer by corrupting files and applications. A virus is a self-replicating program and can copy itself all over the computer system.
Web server	A server that provides web pages to client browsers using the HTTP protocol.

TERM	DESCRIPTION
White-list	A list of USBs or Network devices names that are not considered as dangerous. When a USB\Network device name contains a white-listed entry while scanning a network, GFI LanGuard will ignore the device and consider it as a safe source.
Whois tool	A tool that enables you to look up information on a particular domain or IP address
Wi-Fi	See Wireless LAN
Wireless LAN	A technology used commonly in local area networks. Network nodes use data transmitted over radio waves instead of cables to communicate with each other.
XML	See Extensible Markup Language

16 Appendix - Data Processed by GFI LanGuard

16.1 Introduction

When auditing networks, GFI LanGuard enumerates the information described below, from the specified scan target(s).

16.2 System Patching Status

DATA	DESCRIPTION	PORTS	PROTOCOL
Missing service packs	Discovers missing Microsoft and non-Microsoft service packs	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Missing patches	Discovers missing Microsoft and non-Microsoft patches	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Installed service packs	Lists installed Microsoft and non-Microsoft service packs	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Installed patches	Lists installed and non-Microsoft Microsoft patches	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent

16.3 Ports

DATA	DESCRIPTION	PORTS	PROTOCOL
Open TCP ports	Checks for open TCP ports	All enabled ports in the scan profile	Windows sockets
Open UDP ports	Checks for open UDP ports	All enabled ports in the scan profile	Windows sockets

16.4 Hardware

DATA	DESCRIPTION	PORTS	PROTOCOL
Network devices	Lists physical and virtual network adapters	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Local drives	Lists drives discovered on scanned target(s). Local drives include: » Hard disks » CD/DVD drives » Floppy drives	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Processors	Lists processors discovered during a scan	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Motherboards	Lists motherboards discovered during a scan	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Memory details	Returns memory information of scanned target(s), including: » Total physical memory » Free physical memory » Total virtual memory » Free virtual memory	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Storage details	Lists every storage device discovered during a scan. Storage devices include: » Hard disks » Virtual hard disks » Removable disks » Floppy drives » CD/DVD drives	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Display adapters	Lists video cards discovered during a scan	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI

DATA	DESCRIPTION	PORTS	PROTOCOL
Other devices	Lists generic devices discovered during a scan, including: » System devices/drivers » Human Interface Devices (HID) » Mouse and keyboard » Communication ports (Serial and Parallel) » Floppy disk controllers » Hard disk controllers	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI

16.5 Software

DATA	DESCRIPTION	PORTS	PROTOCOL
General applications	Enumerates every application installed on the scan target(s)	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antispyware applications	Lists antispyware applications	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Patch management applications	Lists patch management applications	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Web browser applications	Lists web browsers	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Firewall applications	Lists firewall applications	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antiphishing applications	Lists antiphishing applications	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
VPN client applications	Lists VPN client applications	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Backup applications	Lists backup applications	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

16.6 System Information

DATA	DESCRIPTION	PORTS	PROTOCOL
Shares	Lists all shares discovered during a scan. Shares information include: » Share name » Share remark » Share path » Share permissions	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Password policy	Lists password policy configuration	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Security audit policy	Security audit policy configuration	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Registry	Lists selected information from the system registry. Amongst others, enumerated information includes: » Registry owner » Current build number » Current type » Current version » Vendor identifier » Software type	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
NetBIOS names	Lists NetBIOS names of the scanned target(s). This node includes: » Workstation service » Domain name » File server services » Browser service elections	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Computer	Lists computer identifiers including: » MAC address » Time to live » Network role » OS Serial number » Language » Machine type (physical or virtual)	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Groups	Lists local or domain/workgroup groups	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

DATA	DESCRIPTION	PORTS	PROTOCOL
Users	Lists local or domain/workgroup users	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Logged on users	Lists locally and remotely logged on users	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Sessions	Lists the active sessions at the time of the scan	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Services	Lists every service discovered during a scan	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Processes	Lists every active process discovered during a scan	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Remote TOD (time of day)	Lists the current time and uptime of the scanned target(s)	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

A

Agent-less audit, 4, 11
Attendant service, 3, 16
Audit result summary, 23
Audit schedule, 6
Auto-remediation, 6, 79

B

Bulletin Info, 28, 125, 126

C

Complete/Combination scans, 77
Custom target properties, 7, 15
CVE, 1, 119, 162, 163, 164, 173

D

deploycmd, 149, 150, 151
Discovery schedule, 6
DNS Lookup, 139, 140, 173

E

Email notifications, 16
Enumerate computers, 139, 143, 144, 174
Enumerate users, 139, 145, 174

H

High security vulnerabilities, 27, 114, 132, 157

I

impex, 149, 151, 152, 164, 174
Import and Export configuration, 97, 98, 99, 100

L

Load scan results, 24
Low security vulnerabilities, 27

M

Management console, 3, 5, 24, 26, 37, 60, 63, 98, 100, 139, 142, 145, 146, 148, 149, 151, 156
Manual audit, 11
Microsoft SQL Server, 4, 89, 148, 174
Missing Patches, 20, 24, 28, 38, 44, 57, 65, 67, 73, 83, 113, 114, 125, 173
Missing service packs, 20, 28, 66, 124

N

NetBIOS, 2, 65, 143, 165
Network & Software Audit, 27, 29, 126
Null session, 13, 53, 68, 70, 73

O

OVAL, 1, 119, 157, 161, 162, 175

P

Potential vulnerabilities, 27, 28
Private key file, 52, 156
Program updates, 93, 95
Proxy settings, 55, 93, 94
Python script, 153, 159, 175

R

Remediation center, 1, 65, 67, 70, 73
Remote desktop connection, 67, 73
Remote Support, 1, 73, 74

S

Save scan results, 25
Scheduled audits, 11
Script Debugger, 3, 154, 175
Security sensors, 1
SMTP Server, 87
SNMP audit, 139, 146
SNMP walk, 139, 147

SQL Server audit, 139, 148, 175

SSH Module, 2, 155, 156

T

Traceroute, 139, 141

U

USB devices, 1, 113, 115, 130, 132

V

VBscript, 2, 153, 155, 175

Vulnerability Assessment, 1, 27, 97, 114,
117, 124, 153, 155

Vulnerability level rating, 24

Vulnerability management strategy, 4

W

Whois, 139, 142, 176

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

ENGLAND AND IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided “as is” with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.